MASTER'S THESIS

Het effect van privacywetgeving

Een exploratief onderzoek naar het effect van privacywetgeving op de implementatie van deze wetgeving bij organisaties

Verver, M. (Mark)

Award date:
2020

Het effect van privacywetgeving

Een exploratief onderzoek naar het effect van privacywetgeving op de implementatie van deze wetgeving bij organisaties

The effect of privacy legislation

An explorative study on the effect of privacy legislation on the implementation of this legislation at organization

Opleiding:	Open Universiteit, faculteit Management, Science & Technology
	Masteropleiding Business Process Management and IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology
	Master Business Process Management & IT
Cursus:	IM9806 Afstudeeropdracht Business Process Management & IT
Student:	Mark Verver
Identiteitsnummer:	
Datum:	4 maart 2020
Afstudeerbegeleider:	Dr. Laury Bollen
Meelezer:	Dr. Rachelle Bosua
Versienummer:	1
Status:	Definitief

I. Abstract

Sinds mei 2018 is de General Data Protection Regulation (GDPR) binnen alle landen van de Europese Unie (EU) van toepassing. Deze verordening stelt eisen aan de manier waarop een organisatie het privacybeleid inricht. Toch bestaat er op dit moment nog discussie over de redenen waarom organisaties kiezen voor een substantiële of symbolische toepassing van deze wetgeving. Enerzijds blijkt dat organisaties gevoelig zijn voor institutionele dwang, aan de andere kant is ook aangetoond dat dwang in veel gevallen leidt tot een symbolische implementatie. In dit document staan de resultaten beschreven van een onderzoek naar de effectiviteit van institutionele dwang doormiddel van wetgeving Dit is gedaan door privacyverklaringen uit 2016 en 2019 van organisaties uit GDPR-gebied, landen met een GDPR-alike wetgeving en andere landen met elkaar te vergelijken. Hieruit is gebleken dat privacyverklaringen wereldwijd sinds de introductie van de GDPR significant in kwaliteit zijn verbeterd. Hierbij is ook gebleken dat de kwaliteit van privacyverklaringen van organisaties uit de EU significant beter zijn dan die uit andere landen. Daarentegen bleek er geen significant verschil te zijn in de kwaliteit van privacyverklaringen uit landen die volgens de EU een degelijke privacywetgeving hebben ten opzichte van organisaties uit andere landen.

II. Sleutelbegrippen

Privacyverklaring, institutionele theorie, substantieel, GDPR

III. Samenvatting

Dit rapport bevat een exploratief onderzoek naar het effect van coërcitieve invloeden van privacygerelateerde wet- en regelgeving op de mate waarin organisaties de privacywetgeving substantieel implementeren. Sinds mei 2018 is de General Data Protection Regulation (GDPR) binnen alle landen van de Europese Unie (EU) van toepassing. Deze wetgeving stelt eisen aan de manier waarop een organisatie het privacybeleid inricht. Hoewel er zware sancties staan op het niet naleven van deze wetgeving, wordt in de literatuur gesuggereerd dat organisaties deze wetgeving in veel gevallen niet substantieel implementeren in het eigen privacybeleid. Enerzijds stellen onderzoekers dat organisaties gevoelig zijn voor institutionele dwang, maar anderzijds is door andere onderzoekers ook aangetoond dat dwang in veel gevallen slechts leidt tot een symbolische implementatie. Met name in een tijd dat mensen zich steeds bewuster worden van hun informatie privacy, is het belangrijk om te weten of deze wetgeving wel het effect heeft dat de beleidsmakers voor ogen hebben of dat dit slechts leidt tot symbolische maatregelen. Het doel van dit onderzoek is om inzicht te krijgen in factoren die van invloed zijn op de mate van substantiële implementatie van privacywetgeving binnen organisaties.

Op dit moment is het nog niet geheel bekend welke factoren van invloed zijn op de keuze van organisaties om privacywetgeving substantieel of slechts symbolisch toe te passen. Wel is er veel onderzoek gedaan naar de substantiële of symbolische toepassing van regelgeving op andere gebieden. Dit onderzoek is grotendeels gebaseerd op de institutionele theorie.

Volgens de institutionele theorie worden organisaties beïnvloed door formele of informele gedragsregels die gelden in de omgeving waarin deze organisaties zich bevinden. Een belangrijk concept binnen de institutionele theorie is isomorfisme, ofwel het idee dat de processen, gedragingen en structuren binnen organisaties in dezelfde omgeving na verloop van tijd gelijkgetrokken worden. Eén van de vormen van isomorfisme is mimetisch isomorfisme. Dit komt voort uit het gedrag van organisaties om de processen en waarden van andere soortgelijke organisaties die volgens de doelorganisatie succesvoller zijn of over een hogere legitimiteit beschikken over te nemen. Een andere vorm van isomorfisme is coërcitief isomorfisme, hetgeen zich uit in bijvoorbeeld dwang door wetgeving zoals de GDPR.

Uit de wetenschappelijke literatuur blijkt dat externe druk, waaronder wet- en regelgeving voor organisaties een belangrijke aanleiding is om het eigen beleid te wijzigen. In het raamwerk voor de institutionele theorie wordt echter ook gesuggereerd dat coërcitief isomorfisme een slechte basis is voor een substantieel privacybeleid omdat beleidsmakers de neiging hebben om enkel dat te doen wat nodig is om een sanctie te voorkomen. Dit onderzoek richt zich voornamelijk op het effect van de GDPR op de kwaliteit van privacyverklaringen van organisaties die aan deze wetgeving moeten voldoen.

Voor dit onderzoek zijn de volgende twee verbanden onderzocht:

1. De invloed van wet- en regelgeving op de mate van substantiële implementatie van deze privacywetgeving bij organisaties;
2. De invloed van het verloop van tijd op de mate van substantiële implementatie van privacywetgeving bij organisaties.

De mate van substantiële implementatie van privacywetgeving is onttrokken uit de privacyverklaring van een organisatie. De organisaties zijn geselecteerd op basis van de volgende drie categorieën:

- Organisaties die aan de GDPR moeten voldoen;

- Organisaties die moeten voldoen aan een privacywetgeving die vergelijkbaar is met de GDPR;
- Organisaties die aan een andere privacywetgeving moeten voldoen.

Voor de eerste hypothese zijn 120 privacyverklaringen uit 2019 getoetst om het effect van de wetgeving te bepalen. Voor tweede hypothese zijn 240 gepaarde privacyverklaringen getoetst om het effect van de factor tijd te bepalen. Tevens is nagegaan of de wetgeving hier een modererende invloed op heeft.

Na het uitvoeren van de statistische toetsen is aangetoond dat organisaties die moeten voldoen aan de GDPR een significant beter privacybeleid hebben dan organisaties die hier niet aan hoeven te voldoen. Uit dezelfde analyse is ook gebleken dat de kwaliteit van de privacyverklaringen van organisaties uit landen met een GDPR-achtige privacywetgeving, niet significant beter is dan die van organisaties uit landen waar dat niet het geval is. Dit terwijl de wetgeving van die landen wel min of meer gelijkwaardig wordt geacht aan de GDPR.

Bewezen is dat de gemiddelde kwaliteit van privacyverklaringen tussen 2016 en 2019 significant is toegenomen. Organisaties die moeten voldoen aan de GDPR laten hierbij de grootste groei zien, terwijl er geen significant verschil is aangetoond tussen de organisaties uit landen waar moet worden voldaan aan een GDPR-achtige privacywetgeving en organisaties die niet aan een strenge privacywetgeving moeten voldoen.

Al met al lijkt het aannemelijk dat coërcitief isomorfisme middels wetgeving leidt tot een kwaliteitsverbetering van privacyverklaringen. Tevens is aangetoond dat de stijging van kwaliteit van privacyverklaringen bij organisaties in de EU samenvalt met de introductie van de GDPR. Daarnaast lijkt er sprake van een zekere vorm van mimetisch isomorfisme tussen de organisaties. Ook organisaties buiten de EU die in de afgelopen drie jaar niet aan strengere privacywetgeving hebben moeten voldoen, hebben gemiddeld genomen een betere privacyverklaring gekregen. Het is hierbij mogelijk dat deze organisaties alsnog de GDPR op enkele vlakken volgen, zonder dat dit nodig is.

Hoewel het niet expliciet is getoetst in de hypothesen, lijkt het erop dat organisaties over het algemeen niet gevoelig zijn voor legitimiteitsaspecten. Slechts een klein deel van de organisaties heeft ervoor gekozen om het voldoen aan sectornormen, gedragsregels of certificaten in de privacyverklaring te communiceren.

IV. Summary

This thesis contains an explorative study on the effect of coercive influences of privacy legislation on the implementation of an organizations' privacy policy. In May 2018, the General Data Protection Regulation (GDPR) was enforced within all European Union (EU) members. This regulation contains a set of privacy related rules that organizations within the EU, or targeting EU citizens need to follow while processing the personal data of their customers. Although the demands of the EU are clear, there is still a lot of ongoing academic discussion whether the enforcement of privacy regulations lead to a substantial implementation or privacy rules, or merely a symbolic one. On one side, it appears that organizations are sensitive to institutional pressure, but on the other hand research on other kinds of regulation has shown that this kind of pressure usually leads to a symbolic implementation. The goal of this research is to gain insight in the factors that have a significant influence of the extend of privacy legislation in an organizations' privacy policy.

Currently it is not yet fully known what factors have a significant influence on the quality of the privacy policy for organizations. However, there has been a lot of research on the factors that have an influence of substantial and symbolic implementation for other fields. Most of this research has focused on the institutional theory.

According to this theory, organizations are under the influence of formal and informal guidelines, that are determined by the organizations' surroundings. One important aspect of the institutional theory is isomorphism. One of the variants of isomorphism is mimetic isomorphism. This means that organizations intentionally or unintentionally copy the behavior of other, often more successful organizations. Another form of isomorphism is coercive isomorphism, of which enforced regulations like the GDPR is an example. According to academic literature, it appears that pressure in the form of legislation often leads to a symbolic implementation of the privacy policy, because managers tend to do minimal investments that are just good enough to avoid sanctions.

The goal of this research is to investigate the following two points:

1. The influence of enforced privacy legislation on the extend of substantial implementation of privacy policies.
2. The influence of world-wide trends in the form of time on the extend of substantial implementation of privacy policies.

To determine the extent of substantial implementation of privacy legislation, the privacy statements of 120 organizations have been graded. These organizations are selected from the following categories:

- Organization that must comply to the GDPR.
- Organizations that must comply to a different kind of privacy legislature that is deemed acceptable by the EU.
- Organizations that must comply to a different kind of privacy legislature that is not deemed acceptable by the EU.

For the first hypothesis 120 privacy statements were selected and tested. For the second hypothesis, 240 paired privacy statements have been analyzed.

After having completed the tests, it has been proven that organizations that are required to comply to the GDPR have a significantly higher quality of privacy statements compared to organizations that need to comply to different kinds of legislation. In the same tests, there did not appear to be a

significant difference in quality of privacy statements when comparing those from countries with a sufficient privacy legislature and those from countries without.

It was also proven that the average quality of privacy statements has grown significantly for all categories between 2016 en 2019. Organizations that need to comply to the GDPR have improved significantly more compared to other organizations. There was no significant difference between organizations that comply another form of sufficient privacy legislation and organizations that don't.

In the end, this research has shown clear signs that coercive isomorphism through legislations is the explanation for the improvement of quality of privacy statements. It also has been proven that organizations that need to comply to the GDPR have shown a significant growth in the quality of privacy statements compared to the other groups. In addition, this research has possible detected a form of mimetic isomorphism because it seems organizations that don't need to comply to the GDPR, seem to have improved the quality of their privacy statements as well.

While not explicitly tested, it seems that organizations are not sensitive to legitimacy. Only a small minority of the organizations seem to communicate their compliance with industry standards, codes of conduct and certificates in their privacy statement.

V. Inhoud

1. Inleiding

Voor u ligt een exploratieve event studie naar het effect van coërcitieve invloeden van privacygerelateerde wet- en regelgeving op de mate waarin organisaties deze wetgeving substantieel implementeren. Tijdens dit onderzoek wordt het effect van de General Data Protection Regulation (GDPR) op het privacybeleid van organisaties onderzocht, door het privacybeleid te vergelijken met dat van organisaties die niet door de GDPR geraakt worden. Dit document vangt eerst aan met een globale verkenning van het onderwerp en een formulering van de opdracht. Vervolgens wordt het theoretisch kader van het onderzoek verkend en wordt de onderzoeksmethode toegelicht. Hierna worden de onderzoeksmethoden beschreven, waaraan ten slotte een conclusie wordt verbonden. Deze scriptie zal afsluiten met een discussie en aanbevelingen voor vervolgonderzoek.

1.1 Privacywetgeving

De Europese Unie (EU) en haar voorlopers proberen al decennialang de privacy van haar ingezetenen te borgen via verdragen en wetgeving. De laatste iteratie van privacywetgeving is de General Data Protection Regulation (GDPR), ook wel Algemene verordening gegevensbescherming (AVG) genoemd. In deze verordening zijn alle plichten beschreven die op het gebied van privacy van toepassing zijn op de verwerkers van persoonsgegevens van natuurlijke personen en de verwerkingsverantwoordelijken (Schermer, Hagenauw, & Falot, 2018). Deze verordening is van toepassing op bijna alle verwerkingsverantwoordelijken van persoonsgegevens die gevestigd zijn op EU-grondgebied, of zich richten op ingezeten van EU-lidstaten. Iedere lidstaat kent vervolgens specifieke bepalingen die zijn vastgesteld in de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Een verwerkingsverantwoordelijke wordt hierbij gezien als het natuurlijk- of rechtspersoon dat verantwoordelijk is voor het vaststellen van het doel en de middelen voor de verwerking van persoonsgegevens.

De GDPR is per 24 mei 2016 in werking getreden en na een transitieperiode van twee jaar wordt deze verordening ook gehandhaafd (Schermer, Hagenauw, & Falot, 2018). Tijdens deze transitieperiode hebben organisaties de kans gekregen om de impact van de GDPR op hun eigen organisatie en processen te bepalen en ze aan deze nieuwe wet aan te passen. Toch is gebleken dat veel organisaties die door de GDPR geraakt zouden worden, pas tegen het einde van deze transitieperiode de eigen processen aanpasten aan de nieuwe eisen. Zo stelt MKB-Nederland dat een groot deel van het midden- en kleinbedrijf (MKB) binnen Nederland vlak voor de toepassingsdatum nog niet klaar was met het nemen van maatregelen om aan de GDPR te voldoen (MKB-Servicedesk, 2018)

Ook de Europese toezichtzichthouders, zoals de Nederlandse Autoriteit Persoonsgegevens (AP) bleken in mei 2018 nog niet helemaal klaar te zijn voor de introductie van de GDPR. Zo zijn er signalen dat de AP kampt met een lage bezetting, waardoor het zich in de eerste instantie slechts zal richten op enkele sectoren (Leupen & Piersma, 2018) (Mebius, 2018). Inmiddels worden er door Europese toezichthouders langzaam de eerste hoge boetes opgelegd wegens GDPR-inbreuken (Alpin, 2019), maar tot nu blijft het nog wachten op grootschalige handhaving vanuit toezichthouders. Verder blijkt dat de AP pas in maart 2019, als een van de eerste toezichthouders in Europa, een concreet beleid heeft vastgesteld voor inbreuken op de UAGV (Autoriteit Persoonsgegevens, 2019), wat het makkelijker zou moeten maken om de UAGV in Nederland te handhaven (Maack, 2019). Het wordt dan ook verwacht dat de GDPR in 2019 door de meeste Europese toezichthouders strenger wordt gehandhaafd (Maack, 2018).

Het niet of onjuist naleven van de GDPR kan leiden tot verschillende sancties, waaronder een door de toezichthouder opgelegde boete van maximaal 10 miljoen euro of wanneer deze hoger is, twee procent van de jaaromzet (Art. 84 GDPR). Toch lijkt het erop dat de GDPR niet altijd even goed wordt nageleefd door alle verwerkingsverantwoordelijken. Ook de Nederlandse overheidsinstanties als de Belastingdienst hebben al voor de toepassingsdatum van de GDPR aangegeven niet te kunnen voldoen aan alle bepalingen wegens de hoeveelheid lastig te onderhouden systemen en een tekort aan medewerkers (Rijksoverheid, 2018).

Buiten het überhaupt niet kunnen voldoen aan alle bepalingen van de GDPR, kan ook de mate van toepassing van de verordening per organisatie verschillen. Dit omdat de GDPR niet expliciet beschrijft hoe de wetgeving geïmplementeerd dient te worden (Spataru-Negura & Lazar, 2018) (Garber, 2018). Sommige organisaties kunnen voor een substantiële implementatie kiezen en stellen daarmee de privacy van de klant centraal. Andere organisaties kunnen juist kiezen voor een symbolische implementatie, waarin enkel het minimale wordt uitgevoerd om maar net, of soms zelfs ogenschijnlijk aan de GDPR te voldoen.

1.2 Probleemstelling

Toch bestaat er op dit moment nog veel discussie over de redenen waarom organisaties kiezen voor een substantiële of juist symbolische toepassing van de wetgeving. Aan de ene kant blijkt dat organisaties gevoelig zijn voor institutionele dwang (Attili, Mathew, & Sugumaran, 2018) (Pollach, 2011), aan de andere kant is ook aangetoond dat dwang in veel gevallen leidt tot een symbolische implementatie (Lannelongue, Gonzalez-Benito, & Gonzalez-Benito, 2013). Met name in een tijd dat mensen steeds zich bewuster worden van hun informatie privacy, is het belangrijk om te weten of wetgeving wel het effect heeft dat de beleidsmakers voor ogen hebben of dat dit slechts leidt tot symbolische maatregelen.

1.3 Doelstelling en relevantie

Het doel van dit onderzoek is om inzicht te krijgen in factoren die van invloed zijn op de mate van substantiële implementatie van de privacywetgeving binnen organisaties. Het onderzoek richt zich voornamelijk op de invloed die de GDPR heeft op de implementatie van deze wetgeving. Tijdens dit onderzoek wordt dan ook de volgende centrale vraag beantwoord:

Wat is de invloed van de General Data Protection Regulation op de mate van substantiële implementatie van deze wetgeving binnen het privacybeleid van organisaties?

Informatie privacy is op dit moment een relatief recent onderwerp (Pavlou, 2011). Toch is de recente inwerkingtreding van de GDPR nog niet heel uitgebreid besproken in de wetenschappelijke literatuur. Hoewel er relatief veel wetenschappelijke literatuur bestaat over factoren die invloed hebben op de keuze om richtlijnen substantieel of symbolisch te implementeren, richt dit zich voornamelijk op keurmerken, milieurichtlijnen en maatschappelijk verantwoord ondernemen in het algemeen (Perez-Batres, Doh, Miller, & Pisani, 2012) (Iatridis & Kesidou, 2018). Dit is een gemis, aangezien juist op het gebied van informatieprivacy, met name door de introductie van de GDPR wereldwijd veel ontwikkelingen plaatsvinden.

Door de centrale vraag van dit onderzoek te beantwoorden kan een verdere stap worden gezet in het bepalen van de noodzaak voor ingrijpende privacygerelateerde wet- en regelgeving, tegenover vertrouwen op privacygerelateerde zelfregulering van organisaties. Daarnaast kan dit onderzoek

gebruikt worden in een grootschaliger onderzoek naar redenen om privacywetgeving substantieel of symbolisch te implementeren.

1.4 Globale opzet

Het doel van dit onderzoek is om de invloed van wet- en regelgeving op de kwaliteit van privacybeleid te bepalen. Om dit te bewerkstelligen wordt allereerst de wetenschappelijke literatuur met betrekking tot dit onderwerp verkend. Hierbij worden de volgende onderwerpen nader onderzocht:

1. Hoe kan beleid als substantieel of symbolisch geclassificeerd worden?
2. Welke wetenschappelijke theorieën kunnen verklaren waarom organisaties ervoor kiezen om beleid te implementeren?
3. Welke wetenschappelijke kennis bestaat er op het gebied van privacy?
4. Wat is de General Data Protection Regulation?
5. Welke wetenschappelijke kennis bestaat er over de koppeling van wetenschappelijke theorieën en de implementatie van privacywetgeving in het privacybeleid?

Aan de hand van de gevonden theorie kunnen er een aantal hypothesen worden gedefinieerd die een uitspraak doen over het effect van privacygerelateerde wet- en regelgeving op de implementatie van privacywetgeving. Aan de hand van de hypothesen wordt vervolgens een onderzoeksmethode vastgesteld. In deze onderzoeksmethode wordt beschreven welke onderzoeksmethode het meest geschikt is voor dit onderzoek, welke gegevens verkregen moeten worden, hoe deze verkregen worden en hoe de gegevens geanalyseerd worden.

Tijdens de analyse wordt er nagegaan wat de invloed van wet- en regelgeving op privacybeleid is door het beleid van twee groepen organisaties te vergelijken: de organisaties die onderhevig zijn aan wet- en regelgeving en de organisaties die dat niet zijn. Door het privacybeleid van dezelfde organisaties te meten kan worden vastgesteld of de eventuele veranderingen veroorzaakt zijn door de inwerkingtreding van strengere privacywetgeving, of dat er andere factoren van invloed kunnen zijn.

2. Theoretisch kader

Om de centrale onderzoeksvraag te kunnen beantwoorden dient er eerst onderzoek te worden gedaan naar de literatuur die over de verschillende onderwerpen beschikbaar is. Volgens Wallace & Wray is een literatuurstudie nodig om te weten te komen wat er op dit moment op wetenschappelijk gebied bekend is met betrekking tot de gestelde onderzoeksvraag. (Wallace & Wray, 2011) In dit hoofdstuk wordt het literatuuronderzoek beschreven naar de verschillende deelvragen. Allereerst wordt het doel en de opzet van het literatuuronderzoek beschreven. Vervolgens wordt er kort gereflecteerd aangaande de uitvoering en worden de resultaten per deelvraag beschreven.

2.1 Onderzoeksaanpak

Saunders, Lewis en Thornhill stellen dat het van belang is om voorafgaand aan het literatuuronderzoek eerst een zoekstrategie te definiëren (Saunders, Lewis, & Thornhill, 2016). Deze strategie zorgt er volgens de schrijvers voor dat de onderzoeker de gemaakte keuzes tijdens de literatuurstudie kan verantwoorden en voorkomt onduidelijkheid met betrekking tot de relevantie van de gekozen literatuur. Deze zoekstrategie zou per onderzoeksvraag het volgende moeten bevatten:

- De zoekparameters;
- De zoeksleutels;
- De databases en zoekmachines die geraadpleegd moeten worden;
- De eigen criteria om relevante en bruikbare onderzoeken voor dit onderzoek te vinden.

Voor het literatuuronderzoek worden eerst de vooraf verstrekte bronnen bestudeerd. Indien relevant, wordt er een combinatie van terug en voorwaarts sneeuwballen gebruikt om gerelateerde bronnen te vinden. Wanneer blijkt dat er informatie over een onderwerp ontbreekt, kan de bouwblok methode worden gebruikt om nieuwe literatuur te verkrijgen. Wanneer hiermee een goede bron is verkregen, kan vervolgens weer een van de sneeuwbal methodes worden gebruikt om hieraan gerelateerde bronnen te vinden. Met alle bronnen kan vervolgens het theoretisch raamwerk verder verdiept worden.

In bijlage A staan de details van de onderzoeksaanpak voor de building blocks methode beschreven.

2.2 Uitvoering

Bij aanvang van de studie zijn er negen geschikte bronnen verstrekt. Vier van deze bronnen hebben betrekking op onderzoek naar de verschillen tussen substantiële en symbolische implementatie van wetgeving. Drie bronnen bevatten literatuurstudies naar informatie privacy. Ten slotte is de wetstekst van de GDPR en een Nederlandse handleiding voor de UAGV verstrekt.

Van deze verstrekte bronnen zijn er in totaal acht gebruikt in het theoretisch kader. De overige 29 bronnen zijn verkregen door een combinatie van backwards snowballing en in mindere mate, de building blocks methode. Er is niet bijgehouden hoeveel gevonden bronnen uiteindelijk niet gebruikt zijn in het onderzoek.

2.3 Gevonden theorie

Hieronder staat de gevonden theorie beschreven.

2.3.1 Redenen tot substantiële en symbolische toepassing

De termen “substantieel” en “symbolisch” zijn in de afgelopen jaren regelmatig gebruikt in relatie tot de implementatie van regulering. Christmann en Taylor definiëren symbolisch en substantieel in hun onderzoek naar de mate van implementatie van de ISO 9000 standaard binnen de industrie bijvoorbeeld als twee uitersten van de implementatie van reguleringsmaatregelen. Hierbij wordt met “symbolisch” het nauwelijks of slechts schijnbaar opvolgen van industriestandaarden bedoeld, terwijl “substantieel” slaat op het herhaaldelijk volledig voldoen aan eisen van deze standaard (Christmann & Taylor, 2006). Volgens Christmann & Taylor kenmerkt een symbolische implementatie zich onder andere door het opstellen van beleid zonder daadkracht om dit beleid ten uitvoer te brengen, terwijl bij een substantiële implementatie de organisatie ervoor zorgt dat het beleid in de praktijk wordt uitgevoerd. In een ander onderzoek definieert Ferrón-Vílchez “symbolische implementatie” als het gebruik van een keurmerk of industriestandaard om steun te vergaren onder een groep stakeholders, zonder zich daadwerkelijk in te zetten om deze substantieel te implementeren (Ferrón-Vílchez, 2016).

Op dit moment is het nog niet geheel duidelijk of er factoren zijn die invloed hebben op de keuze van organisaties om privacygerelateerde wet- en regelgeving substantieel of slechts symbolisch toe te passen. Wel is er veel onderzoek gedaan naar de substantiële of symbolische toepassing van regelgeving op andere gebieden. De reden dat organisaties ervoor kiezen om wet- en regelgeving substantieel of symbolisch toe te passen kan gevonden worden in meerdere theorieën, waarvan de volgende vaak voorkomen in academische literatuur (Fernando & Lawrence, 2014):

- Institutionele theorie;
- Legitimiteitstheorie;
- Stakeholder theorie.

Institutionele theorie

Volgens de institutionele theorie worden organisaties beïnvloed door formele of informele gedragsregels die geldig zijn in de omgeving waarin organisaties zich bevinden (DiMaggio & Powell, 1983) (Greenwood & Meyer, 2008). Een belangrijk concept binnen de institutionele theorie is isomorfisme, ofwel het idee dat de processen, gedragingen en structuren binnen organisaties in dezelfde omgeving na verloop van tijd gelijkgetrokken worden (DiMaggio & Powell, 1983). Binnen dit concept worden door DiMaggio & Powell de volgende drie vormen van isomorfisme onderkend:

- Coërcitief isomorfisme;
- Mimetisch isomorfisme;
- Normatief isomorfisme.

Coërcitief isomorfisme wordt volgens de auteurs veroorzaakt door druk vanuit andere partijen, zoals ketenpartners of overheden, waarvan de organisatie afhankelijk is, of vanuit de samenleving als een geheel. Een voorbeeld van deze druk is het aanpassen van de eigen processen om te kunnen voldoen aan de geldende wet- en regelgeving. Doordat het niet voldoen aan wetgeving veelal nadelige gevolgen met zich meebrengt, zullen veel organisaties ervoor kiezen om deze op te volgen (Clemens & Douglas, 2006). Omdat wet- en regelgeving voor een grotere omgeving geldt, zullen alle getroffen organisaties de betreffende processen op een soortgelijke manier inrichten (DiMaggio & Powell, The iron cage revisited: Institutional isomorphism and collective rationality in organizations., 1983). Er worden verschillende aanleidingen onderkend die kunnen leiden tot coërcitief isomorfisme. Twee daarvan zijn oplegging en aansporing (Scott, 1987). Het verschil tussen deze twee aanleidingen ligt

volgens Scott met name in de macht van de partij die de wijziging in gedrag bij de organisatie teweeg wil brengen. Een partij die macht kan uitoefenen, bijvoorbeeld een overheid kan verandering afdwingen terwijl een partij met minder macht een organisatie hoogstens kan verzoeken om een verandering teweeg te brengen. Volgens Scott (1987) lijkt het er daarnaast op dat de kans klein is dat aansporing leidt tot een blijvende verandering bij de doelorganisatie.

Mimetisch isomorfisme komt daarentegen voort uit het gedrag van organisaties om de processen en waarden van andere soortgelijke organisaties die volgens de doelorganisatie succesvoller zijn of over een hogere legitimiteit beschikken over te nemen (DiMaggio & Powell, 1983). Dit gedrag komt volgens Cyert & March met name voor bij organisaties die zelf moeite hebben met het oplossen van een specifiek intern probleem (Cyert & March, 1963) (Argote & Greve, 2007). Dit type isomorfisme vindt meestal plaats zonder dat de bronorganisatie daar invloed op heeft, bijvoorbeeld door personeel aan te nemen dat bij de bronorganisatie werkzaam is geweest of door het inzetten van dezelfde consultancybureaus (DiMaggio & Powell, 1983). Een van de manieren om mimetisch isomorfisme in gang te zetten is de bewuste keuze van organisaties om bepaalde gedragingen en structuren aan te nemen (Scott, 1987). Omdat de organisatie zelf de bewuste keuze maakt om bepaalde gedragingen over te nemen, stelt Scott dat de organisatie zich meestal meer inzet om deze veranderingen substantieel door te voeren dan wanneer deze veranderingen opgelegd of aangespoord worden.

Ten slotte komt normatief isomorfisme voort uit de professionele samenwerking tussen gelijkgestemden binnen dezelfde organisatie, die invloed uitoefenen op de waarden en processen binnen de betreffende organisatie (DiMaggio & Powell, The iron cage revisited: Institutional isomorphism and collective rationality in organizations., 1983) (Magali, Sarfatti, & Larson, 1977). Volgens DiMaggio & Powell wordt dit type isomorfisme voornamelijk veroorzaakt door scholing, kennisdeling in professionele netwerken en het selecteren van nieuwe medewerkers op dezelfde, stereotype kenmerken. Een manier om normatief isomorfisme te initiëren bij een organisatie is het verkrijgen van gedragingen. De organisatie wordt hierbij door een controlerende partij niet verplicht om bepaalde gedragingen te uiten, maar doet dit vrijwillig en op eigen initiatief om zo een bepaalde legitimiteit te verkrijgen (Scott, 1987).

Legitimiteitstheorie

Een andere theorie die de keuze voor symbolische of substantiële implementatie kan verklaren is de legitimiteitstheorie. Legitimiteit kan worden gedefinieerd als: *"…a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions"* (Suchman, 1995). Suchman stelt dat er twee dimensies bestaan waarover het streven van legitimiteit kan worden gemeten:

- Het streven naar continuïteit en geloofwaardigheid;
- Het zoeken naar actieve steun versus het zoeken naar passieve steun.

De legitimiteit van een organisatie heeft een positieve invloed op de continuïteit van de organisatie omdat klanten de voorkeur hebben om hun bronnen, zoals tijd en geld te bieden aan organisaties die authentiek, gewild of fatsoenlijk overkomen (Suchman, 1995) (Parsons, 1960). Tegelijkertijd heeft legitimiteit niet alleen invloed op de manier waarop klanten zich gedragen naar een organisatie, maar ook op de manier waarop klanten deze organisatie zien (Meyer & Rowan, 1991).

Daarnaast kan de mate van legitimiteit van een organisatie worden bepaald aan de hand van de mate waarin een organisatie op zoek is naar een actieve ondersteuning van klanten. Een organisatie die slechts zoekt naar minimale interactie van een klant, bijvoorbeeld enkel het doen van een enkele transactie, hoeft niet over veel legitimiteit te beschikken. Wanneer een organisatie echter een

langdurige relatie met een klant wil aangaan, stelt de klant hogere eisen aan de legitimiteit van de organisatie (DiMaggio, 1988).

Stakeholder theorie

De laatste theorie waarmee verklaard kan worden waarom organisaties bepaalde regelgeving substantieel of symbolisch toepassen is de stakeholder theorie. Volgens Freeman en Reed zijn stakeholders groepen of individuen die invloed uitoefenen op het behalen van de doelen van een organisatie, of die invloed ondervinden door het behalen van de doelen van een organisatie (Freeman & Reed, 1983). Pérez-Batres et al. vatten deze theorie samen door te stellen dat organisaties niet alleen handelen naar het belang van de aandeelhouder of eigenaar, maar naar de gehele groep stakeholders van de organisatie. De invloed van alle stakeholders binnen een organisatie zou vervolgens zorgen voor een efficiëntere besturing van deze organisatie. Het effect van stakeholders op een organisatie zou beïnvloed kunnen worden door een boodschap uit te dragen die deze groep aanspreekt (Perez-Batres, Doh, Miller, & Pisani, 2012). Uit het onderzoek van Perez-Batres et al. naar de implementatie van Corporate Social Responsibility (CSR) maatregelen, blijkt dat alleen de invloed van bepaalde groepen stakeholders gevolgen heeft op de keuze van een organisatie om deze maatregelen substantieel of symbolisch toe te passen.

2.3.2 Privacy

Uit diverse onderzoeken blijkt dat Informatieprivacy een steeds belangrijker onderwerp lijkt te worden (Bélanger & Crossler, 2011). Hoewel Informatieprivacy een breed en complex begrip is, kan het in grote lijnen worden gedefinieerd als het concept dat iemand zelf kan bepalen welke persoonlijke informatie vergaard en gebruikt wordt (Pavlou, 2011) (Stone, Gueutal, Gardner, & McClure, 1983). Wat privacy dan precies is, is een discussie die nog loopt (Smith, Dinev, & Xu, 2011). Volgens Smith, Dinev & Xu zien sommige onderzoekers het als een onaantastbaar recht, anderen als een verhandelbaar goed. Weer andere onderzoekers zien privacy als een staat waarin iemand kan verkeren, of juist een middel om een ander doel, zoals autonomie te behalen (Westin, 1967). Smith, Dinev & Xu geven in ieder geval aan dat privacy geen synoniem is voor concepten als anonimiteit, geheimhouding, vertrouwelijkheid, veiligheid en ethiek.

Consumentenvertrouwen en legitimiteit

Privacy is volgens Smith, Dinev en Xu een vaak onderzochte variabele. Zo lijkt de mate waarin consumenten waarde hechten aan privacy, volgens Smith, Denev & Xu afhankelijk te zijn van de afweging tussen het risico van het verlies van privacy en de voordelen van het vrijwillig opgeven van een deel van de privacy voor de betreffende individuen (Smith, Dinev, & Xu, 2011). Daarnaast blijkt er een verband te zijn tussen het consumentenvertrouwen in een website en de mate waarin de betreffende website de indruk wil wekken om privacyvriendelijk te opereren (Smith, Dinev, & Xu, 2011). Dit consumentenvertrouwen kan uiteindelijk een mediërende factor zijn tussen de waarde die iemand hecht aan de eigen privacy en de bereidheid om een transactie aan te gaan (Eastlick, Lotz, & Warrington, 2006). Er kan dus worden gesteld dat organisaties die wat betreft privacy een hoog consumentenvertrouwen opwekken, een hogere kans hebben om transacties aan te gaan met consumenten.

Het is echter niet altijd nodig om een gedegen privacybeleid substantieel te implementeren om consumentenvertrouwen te verkrijgen. Zo blijkt uit onderzoek van Miyazaki & Krishnamurthy dat consumenten positiever tegenover het privacybeleid van organisaties staan, wanneer de desbetreffende organisatie zichtbare privacygerelateerde logo's op de website toont, zonder dat deze logo's ook een werkelijke betekenis hebben (Miyazaki & Krishnamurthy, 2002).

Roep om regulering

Tegelijkertijd blijkt dat consumenten organisaties meer wantrouwen wanneer zij het gevoel krijgen dat organisaties hun privacy niet voldoende respecteren. In dat geval verliezen consumenten het vertrouwen in de zelfregulering van organisaties en gaat de voorkeur uit naar institutionele druk middels wet- en regelgeving (Milberg, Smith, & Burke, 2000). Ten slotte blijkt dat inwoners van landen met strenge privacywetten meer de neiging hebben om voorstander te zijn van nog strengere overheidsgestuurde regulering (Bellman, Johnson, Kobrin, & Lohse, 2004). Hieraan gerelateerd blijkt uit het literatuuronderzoek van Bélanger en Crossler dat overheidsinterventie een mediërende invloed heeft op wisselwerking tussen de privacyzorgen die een individu uit, en de privacyzorgen van de gehele samenleving (Bélanger & Crossler, 2011).

Over de effectiviteit van privacyregulering is veel onderzoek gedaan. Een voorbeeld is het onderzoek van Birnhack en Elkin-Koren naar de mate van compliance van websites met betrekking tot de geldende privacywetgeving. Zij constateerden dat er een groot verschil bestaat tussen de populariteit van de website en de mate van compliance. Hoewel de meest populaire websites, of websites van organisaties die veel persoonsgegevens verwerken voor een groot deel compliant zijn met de wetgeving, bleef de compliancy van de minder populaire websites flink achter (Birnhack & Elkin-Koren, 2011). Een mogelijke reden hiervoor is volgens Birnhack en Elkin-Koren dat de grotere websites een hoger budget hebben om juridisch advies in te winnen, eerder wordt gecontroleerd door privacygerelateerde toezichthouders en harder worden geraakt door eventuele sancties dan de websites van kleinere organisaties. Tevens constateerden de onderzoekers dat privacywetgeving alleen maar effectief is wanneer de overheid een krachtige toezichthouder aanstelt die over voldoende mandaat beschikt, de middelen heeft om sancties op te leggen en over de capaciteit beschikt om de privacywetgeving te handhaven. In andere gevallen zijn zelfregulering of druk vanuit stakeholders effectievere methoden om de privacy van klanten ten beschermen (Birnhack & Elkin-Koren, 2011).

2.3.3 De GDPR

Een van de meest recente ontwikkelingen op het gebied van privacywetgeving is de Data Protection Regulation (GDPR) en de Nederlandse implementatie daarvan: de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) (Schermer, Hagenauw, & Falot, 2018). De GDPR is van toepassing op alle organisaties die binnen de Europese Unie (EU) gevestigd zijn, of gegevens verwerken van ingezetenen van de EU. Organisaties buiten de EU, die geen gegevens van EU-ingezetenen verwerken zijn dus niet verplicht om aan de GDPR voldoen.

De GDPR is een vervanger van de hiervoor geldende Data Protection Directive 95/46/EC (DIR95) (Tikkinen-Piri, Rohunen, & Markkula, 2018). Volgens Tikkinen-Pri, Rohunen & Markkula verschilt de GDPR op de volgende vlakken van de DIR95. De meest grote verschillen zijn in bijlage B opgenomen.

Tegen het niet opvolgen van de GDPR staan hoge boetes (Schermer, Hagenauw, & Falot, 2018), maar toch blijkt uit onderzoek dat bijna een jaar na de inwerkingtreding van de GDPR, veel organisaties die door deze wetgeving worden geraakt niet geheel aan deze wetgeving voldoen (MacMillan, 2019; Davies, 2018). MacMillan en Perry geven verder aan dat organisaties die niet aan de GDPR voldoen, hiervoor verschillende redenen hebben, zoals een gebrek aan tijd, kennis of budget (Perry, 2019) (MacMillan, 2019). Een van de grotere vraagstukken voor organisaties uit het Verenigd Koninkrijk is de uittreding uit de Europese Unie. Door deze zogenaamde Brexit vraagt men zich binnen veel Britse organisaties af of men nog moet voldoen aan de GDPR en zo niet, wat voor alternatieve privacywetgeving wordt opgesteld door de Britse regering.

Reacties van grote commerciële dataverwerkers

Een van de gevolgen van de introductie van de GDPR is het vereisen van toestemming van betrokkenen, om gegevens te mogen verwerken (Tikkinen-Piri, Rohunen, & Markkula, 2018). Dit heeft uiteindelijk tot gevolg dat organisaties actief gebruikers proberen te overtuigen om gegevens te laten verwerken. Een voorbeeld is bijvoorbeeld de methode van Facebook. Wanneer een gebruiker de toestemming voor gezichtsherkenning in de privacyvoorkeuren aanpast, wordt deze gewaarschuwd dat de gebruiker zichzelf ook niet meer automatisch kan laten 'taggen' op foto's van Facebookvrienden (Davies, 2018). Ditzelfde beeld ontstaat ook bij organisaties als Microsoft en Google, die gebruikers proberen te verleiden tot het verstrekken van extra persoonsgegevens door argumenten aan te voeren die in het voordeel van de gebruiker lijken te zijn, zonder transparant te zijn over de voordelen voor de organisatie zelf.

Een ander, wellicht onbedoeld, effect van de introductie van de GDPR is dat grote commerciële dataverwerkers zoals Facebook stappen ondernemen om juist data van niet-Europese gebruikers buiten de EU te verplaatsen (Davies, 2018). Een mogelijke verklaring voor deze dataverhuizing is volgens Davies dat de persoonsgegevens onder strenge privacywetgeving als de GDPR voor een organisatie die afhankelijk is van advertentie-inkomsten, commercieel minder waardevol is als persoonsgegevens die onder minder strenge wetgeving vallen.

Eerste adviezen voor substantiële implementatie

Langzaam maar zeker komt er meer literatuur beschikbaar met als onderwerp de implementatie van de GDPR. Perry adviseert de volgende stappen (Perry, 2019):

- Inventariseer alle beschikbare documentatie met betrekking tot dataverwerking en breng alle verwerkingen in kaart. Wijs indien nodig een functionaris voor gegevensbescherming aan die dit kan coördineren.
- Blijf op de hoogte over nieuws en informatie vanuit de toezichthouden en de European Data Protection Board zodat de organisatie op de hoogte is van de exacte eisen aan het verwerken van persoonsgegevens. De organisatie kan vervolgens zelf inschatten welke veranderingen nog moeten worden doorgevoerd om volledig aan de GDPR te voldoen.
- Zorg dat alle personeelsleden en met name de dataverwerkers op de hoogte zijn van de eisen die de GDPR aan gegevensverwerking stelt. Dit zorgt er volgens Perry voor dat gegevensbescherming meer gaat leven onder de medewerkers.

Deze maatregelen zouden volgens Perry voorkomen dat het implementeren van privacymaatregelen wordt gereduceerd tot het symbolisch voldoen aan de GDPR.

2.3.4 Invloed van oplegging op de implementatie van privacywetgeving

Privacybeleid wordt vaak gezien als een vorm van Corparate Social Responsibility (CSR). Volgens Carroll wordt er van organisaties verwacht dat zij aan de volgende vier voorwaarden voldoen: zij moeten financieel gezond zijn, zich aan de wet houden, via filantropie iets teruggeven aan de maatschappij en zich ethisch gedragen (Carroll, 1998). Pollach stelt dat het bewaken van de informatieprivacy van klanten gezien kan worden als ethisch gedrag (Pollach, 2011). Dit wil echter niet zeggen dat organisaties alleen privacymaatregelen nemen uit ethische overwegingen. Uit onderzoek van Aguilera, Rupp, Williams en Ganapathi blijkt dat er drie belangrijke motivaties kunnen worden aangewezen die organisaties ertoe bewegen om privacyvriendelijk beleid toe te passen (Aguilera, Rupp, Williams, & Ganapathi, 2007). Dit zijn:

- De morele overtuigingen van de organisatie of de personen die verantwoordelijk zijn voor het privacybeleid.

- Invloeden van buitenaf, zoals druk vanuit stakeholders.
- De eigen zakelijke belangen van de organisatie, zoals het voldoen aan coërcitieve druk om sancties vanuit privacygerelateerde toezichthouders en overheden te voorkomen.

Ten tijde van het onderzoek van Aguilera, waren met name de eigen zakelijke belangen de sterkste motivatie om CSR-maatregelen te implementeren. Dit terwijl Burke & Logsdon stellen dat om CSR-maatregelen substantieel te implementeren, de maatregelen dicht bij de missie van organisatie moeten staan en dat de organisatie uit eigen initiatief voor deze maatregelen kiest (Burke & Logsdon, 1996).

Dit lijkt in lijn met de stelling van Scott dat de kans klein is dat de coërcitieve oplegging van nieuwe processen en structuren leidt tot blijvende veranderingen (Scott, 1987). Uit een case study naar de invloed van verschillende soorten isomorfisme op de privacystrategie van enkele IT-organisaties blijkt echter dat het hoger management meer gevoelig is voor coërcitieve invloeden, dan voor normatieve en mimetische invloeden (Attili, Mathew, & Sugumaran, 2018). Tegelijkertijd constateren Attili, Mathew & Sugumaran dat de steun vanuit het hoger management een mediërende invloed heeft op de relatie tussen coërcitief isomorfisme en de implementatie van privacywetgeving, terwijl de organisatiecultuur en bekwaamheid op het gebied van privacy een modererende invloed op hetzelfde verband heeft. Een van de beperkingen van dit onderzoek is dat zoals eerder benoemd, een wijziging van de privacystrategie niet per sé hoeft te leiden tot een substantiële implementatie van privacywetgeving, hooguit geeft dit slechts de intentie aan. In een ander onderzoeksgebied zijn Zailani, Eltayeb, Hsu & Tan tot de conclusie gekomen dat organisaties ook gevoelig zijn voor externe druk om hun producten milieuvriendelijker te produceren (Zailani, Eltayeb, Hsu, & Tan, 2012), maar geven Lannelongue, Gonzalez-Benito & Gonzalez-Benito dat externe druk niet altijd voldoende is om dit beleid ook op een substantiële manier uit te voeren (Lannelongue, Gonzalez-Benito, & Gonzalez-Benito, 2013).

Toch lijkt het beeld dat organisaties gevoelig zijn voor externe druk om privacymaatregelen te nemen te worden bevestigd door een eerder uitgevoerd onderzoek door Pollach. Hieruit komt naar voren dat in het pre GDPR-tijdperk weinig binnen Europa opererende organisaties op eigen initiatief beschikken over een concreet en substantieel privacybeleid (Pollach, 2011). Ten slotte stelt ook Edelman dat consumenten het gevoel hebben dat privacymaatregelen bij organisaties beter worden geïmplementeerd wanneer deze vanuit buitenaf opgelegd worden, dan wanneer deze middels zelfregulering tot stand komen (Edelman, 2011).

2.4 Doel van het vervolgonderzoek

Uit de wetenschappelijke literatuur blijkt dat externe druk, waaronder wet- en regelgeving voor organisaties een belangrijke aanleiding is om een gedegen privacybeleid op te zetten (Pollach, 2011) (Attili, Mathew, & Sugumaran, 2018). In het raamwerk voor de institutionele theorie wordt echter gesuggereerd dat coërcitief isomorfisme in de vorm van dwang of druk een slechte basis is voor een substantieel privacybeleid omdat managers de neiging hebben om een minimale investering te doen die nodig is om een sanctie te voorkomen (DiMaggio & Powell, 1983) (Scott, 1987). Daarentegen stelt Scott dat mimetisch en normatief isomorfisme vaker leidt tot een substantiële implementaties, omdat managers hierbij uit eigen initiatief het privacybeleid aanpassen om mee te komen met concurrenten of om legitimiteit te verkrijgen bij consumenten (Scott, 1987) (Meyer & Rowan, 1991) .

Dit onderzoek zal zich voornamelijk richten op de invloed van de privacy gerelateerde wet- en regelgeving waaraan een organisatie onderhevig is op de mate waarin de betreffende organisatie de

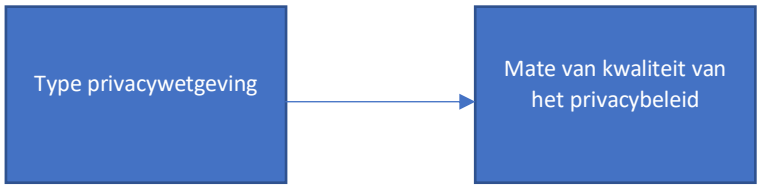
privacy van haar consumenten wil borgen. Daarnaast wordt onderzocht in hoeverre het verloop van tijd invloed heeft gehad op de mate van kwaliteit van het privacybeleid van organisaties die wel of niet onderhevig zijn aan strenge, privacy-gerelateerde wet- of regelgeving. Dit om te onderzoeken wat de invloed van normatieve invloeden zoals veranderende sectornormen of mimetische invloeden zoals algemene ontwikkelingen op privacygebied is.

2.4.1 Hypotheses

Er wordt onderzoek gedaan naar de volgende hypothesen:

H1: *Een organisatie die onderhevig is aan strenge privacy-gerelateerde wet- of regelgeving beschikt over een privacybeleid van betere kwaliteit dan organisaties die niet aan strenge privacy-gerelateerde wet- en regelgeving moeten voldoen.*

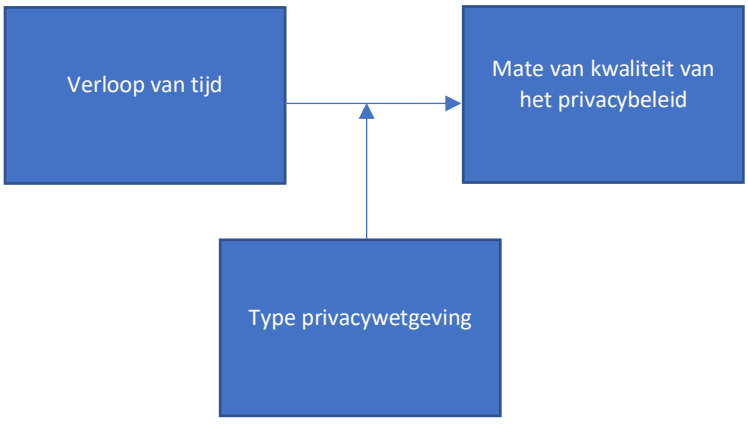
Voor de eerste hypothese wordt een cross-sectioneel onderzoek uitgevoerd naar het effect van het type privacywetgeving op de mate van kwaliteit van de privacyverklaring.



Figuur 1: Hypothese 1, effect wet- en regelgeving op privacybeleid

H2: *De privacyverklaring van organisaties die onderhevig zijn geweest aan strengere privacy-gerelateerde wet- of regelgeving is na verloop van tijd privacyvriendelijker geworden dan bij organisaties die in dezelfde periode niet onderhevig zijn geweest aan strengere privacy-gerelateerde wet- of regelgeving.*

Voor de tweede hypothese wordt een longitudinaal onderzoek uitgevoerd naar het effect van verloop van tijd op de mate van kwaliteit van de privacyverklaring. Ook wordt ook getoetst of het type privacywetgeving een modererende invloed heeft gehad op de mate waarin de kwaliteit van privacyverklaringen na verloop van tijd is gewijzigd.



Figuur 2: Hypothese 2, effect verloop van tijd op privacybeleid

3. Methodologie

Voor dit onderzoek worden de volgende twee verbanden onderzocht:

- De invloed van wet- en regelgeving op de mate van substantiële implementatie van privacywetgeving bij organisaties;
- De invloed van het verloop van tijd op de mate van substantiële implementatie van privacywetgeving bij organisaties.

Om dit onderzoek uit te kunnen voeren moet allereerst bepaald worden op welke manier de implementatie van het privacybeleid beoordeeld kan worden. Ten tweede moeten organisaties ingedeeld worden in een groep organisaties die getroffen wordt door de GDPR, een groep die niet geraakt wordt door de GDPR maar wel door een andere strenge privacywetgeving en een groep die niet geraakt wordt door strenge privacywetgeving. Ten slotte moet er een manier gevonden worden om na te gaan wat de invloed van wereldwijde trends op het gebied van privacy in de vorm van het verloop van tijd is op het privacybeleid van organisaties.

3.1 Mate van substantiële implementatie

De mate van substantiële implementatie van privacywetgeving kan worden onttrokken uit de privacyverklaring van de organisatie. Deze privacyverklaring bevat over het algemeen informatie waarom een organisatie, welke persoonsgegevens verwerkt, hoe deze verwerking plaatsvindt en hoelang de gegevens opgeslagen blijven staan. Dit brengt enkele voor- en nadelen met zich mee. Enerzijds beschikken veel organisaties over een privacyverklaring en kunnen deze snel geanalyseerd en beoordeeld worden, waardoor de totale dataset voor dit onderzoek van voldoende omvang is om tot een goed onderbouwde conclusie te komen. Anderzijds is een van de beperkingen dat de intenties die in de privacyverklaring staan beschreven geen bewijs zijn voor de manier waarop de organisatie het beleid daadwerkelijk uitvoert (Smith, Dinev, & Xu, 2011) (Pollach, 2011). Middels de theorie van beredeneerde actie zoals deze is gedefinieerd door Fishbein & Ajzen kan worden gesteld dat intentie veelal leidt tot getoond gedrag (Yousafzai, Foxall, & Pallister, 2010) (Fishbein & Ajzen, 1975). Hierbij dient wel opgemerkt te worden dat de intentie volgens de theorie van beredeneerde actie wordt beïnvloed door iemands houding, waarden, ideeën of visie, terwijl een privacyverklaring ook is opgesteld met het oog op andere organisatiebelangen zoals wet- en regelgeving, het vergroten van legitimiteit of druk vanuit stakeholders. Hoewel er goede redenen zijn om de privacyverklaring van organisaties te analyseren, blijft ontbreken van bewijs voor daadwerkelijk gedrag wel een beperking bij dit onderzoek.

3.1.1 Organisaties onder invloed van wet- en regelgeving

Allereerst moeten er organisaties gevonden worden die hun beleid hebben moeten aanpassen in verband met strenge wet- en regelgeving. Hiervoor kunnen organisaties gebruikt worden die binnen de Europese Unie (EU) actief zijn omdat deze onder de GDPR vallen. Ten behoeve van de uitvoerbaarheid van het onderzoek worden alleen die organisaties geselecteerd die hun privacyverklaring in de Nederlandse of Engelse taal beschikbaar hebben gesteld. Dit kan enkele nadelen met zich meebrengen: Ten eerste kan het voorkomen dat ongeacht de geldende wetgeving, er normatieve verschillen bestaan tussen het beeld dat in verschillende taalgebieden of landen gebruikelijk is ten opzichte van privacy. Door dit onderzoek alleen op Nederlandstalige en Engelstalige organisaties te richten kan dit verschil onzichtbaar blijven. Daarnaast kan het voorkomen dat met name multinationale organisaties met een Engelstalige privacyverklaring buiten het Engelstalig taalgebied qua omzet, aantal personeelsleden en doelgroep dusdanig afwijkt van een

‘gemiddelde’ organisatie dat deze factoren ook invloed hebben op de mate van substantiële implementatie. Hier zal in het onderzoeksontwerp rekening mee worden gehouden.

Ten tweede moeten er organisaties geselecteerd worden die niet onder strenge privacy wet- en regelgeving vallen. Ook hier gaat de voorkeur uit naar Engelstalige organisaties om het analyseren van de privacyverklaring te vergemakkelijken. Daarnaast mag de organisatie geen persoonsgegevens van natuurlijke personen binnen de EU verwerken, omdat deze organisatie dan ook aan de GDPR zou moeten voldoen (Schermer, Hagenauw, & Falot, 2018). Er komen ook geen landen in aanmerking die volgens de EU een voldoende strenge privacywetgeving kennen. Dit zijn (Autoriteit Persoonsgegevens, sd):

- Andorra
- Argentinië
- Canada (commerciële organisaties)
- Faeröer Eilanden
- Guernsey
- Isle of Man
- Israël
- Japan
- Jersey
- Nieuw-Zeeland
- Uruguay
- Zwitserland
- Verenigde Staten (enkel de organisaties die onder de Privacy Shield regeling vallen en luchtvaartmaatschappijen)

Ook de overzeese landen en gebieden van EU-landen zijn niet meegenomen, omdat het aannemelijk is dat deze een deel van de privacywetgeving van het land waar zij aan verbonden zijn hebben overgenomen.

Ten slotte kan er ook een groep grote of middelgrote Nederlands- of Engelstalige landen worden geselecteerd die niet aan de GDPR hoeven te voldoen, maar volgens de EU wel een voldoende beschermende privacywetgeving hanteren. Ook het privacybeleid van organisaties die opereren binnen deze landen kan vergeleken worden met dat van organisaties die geraakt worden door de GDPR en dat van organisaties die door geen enkele strenge privacywetgeving geraakt worden.

Dit zijn:

- Canada (mits voor commerciële organisaties)
- Nieuw-Zeeland
- Verenigde Staten (enkel de organisaties die onder de Privacy Shield regeling vallen en luchtvaartmaatschappijen)

Ook van deze organisaties moet het aannemelijk zijn dan zij geen persoonsgegevens van EU-ingezetenen verwerken, omdat de organisatie dan aan de GDPR moet voldoen.

3.1.2 Invloed van wereldwijde ontwikkelingen na verloop van tijd

Om dit te meten wordt er geprobeerd om van iedere organisatie een privacyverklaring te vinden die op dit moment geldig is en een verklaring die tot de introductie van de GDPR, op 24 mei 2016, geldig was. Door deze te vergelijken met organisaties die wel of niet geraakt zijn door de GDPR, kan vastgesteld worden of de veranderingen in het privacybeleid niet ook op een andere manier dan de oplegging van wet- en regelgeving doorgevoerd hadden kunnen worden.

Deze oude versies van privacyverklaringen kunnen op de volgende manieren verkregen worden:

- Uit een openbaar archief op de website van de te onderzoeken organisatie;

- Middels een historische zoekmachine waarmee snapshots van pagina's inzichtelijk worden gemaakt, zoals The Wayback Machine;
- Door deze op te vragen bij de betreffende organisatie.

3.1.3 Gekozen onderzoeksmethode

Om een grote hoeveelheid privacyverklaringen te analyseren kan er gekozen worden voor een kwantitatieve onderzoeksmethode. Deze is volgens Saunders, Lewis & Thornhill geschikt om verbanden tussen verschillende variabelen te onderzoeken middels gekwantificeerde gegevens (Saunders, Lewis, & Thornhill, 2016). Het voordeel van deze onderzoeksmethode is dat relatief grote datasets snel inzichtelijk kunnen worden gemaakt om zo een hypothese te toetsen. Om de privacyverklaringen te kunnen kwantificeren kunnen deze beoordeeld worden op de mate van privacyvriendelijke implementatie.

3.2 Technisch ontwerp: uitwerking van de methode

In dit onderdeel worden de details van de gekozen onderzoeksmethode beschreven.

3.2.1 Selectie organisaties

Zoals hiervoor beschreven is, worden er zowel organisaties geselecteerd die geraakt worden door de GDPR-wetgeving en organisaties die dat niet worden. Omdat het binnen dit onderzoek niet praktisch is om willekeurige organisaties te selecteren, worden deze middels enkele selectiecriteria geselecteerd.

De organisaties die door de GDPR worden geraakt moeten aan de volgende voorwaarden voldoen:

Tabel 1: Voorwaarden GDPR-organisaties

Voorwaarde	Motivatie
De organisatie moet zich op EU-grondgebied bevinden of persoonsgegevens van EU-ingezetenen verwerken.	Alleen deze organisaties moeten aan de GDPR voldoen.
De organisatie moet een Nederlands- of Engelstalige privacyverklaring op de eigen website hebben gepubliceerd.	Dit om de analyse te vergemakkelijken.

De organisaties die niet geraakt worden door strenge privacywetgeving, moeten aan de volgende voorwaarden voldoen:

Tabel 2: Voorwaarden niet GDPR-alike organisaties.

Voorwaarde	Motivatie
De organisatie moet zich niet op EU-grondgebied bevinden of de persoonsgegevens van EU-ingezetenen verwerker.	Deze organisaties hoeven niet aan de GDPR te voldoen.
De organisatie moet een Nederlands- of Engelstalige privacyverklaring op de eigen website hebben gepubliceerd.	Dit om de analyse te vergemakkelijken.
De organisatie komt niet uit een land met een door de EU goedgekeurde privacywetgeving.	Deze organisatie vallen niet onder een privacywetgeving die door de EU als voldoende streng wordt beschouwd.
De organisatie bevindt niet in een overzees gebied van een EU-land.	De kans is groot dat overzeese gebieden alsnog delen van de privacywetgeving van het land waaraan deze verbonden is overneemt.

De organisaties die niet door de GDPR worden geraakt, maar wel aan een privacywetgeving moeten voldoen die met de GDPR vergelijkbaar is:

Tabel 3: Voorwaarden GDPR-alike organisaties.

Voorwaarde	Motivatie
De organisatie moet een Nederlands- of Engelstalig privacyverklaring op de eigen website hebben gepubliceerd.	Dit om de analyse te vergemakkelijken.
De organisatie moet zich niet op EU-grondgebied bevinden of de persoonsgegevens van EU-ingezetenen verwerker.	Deze organisaties hoeven niet aan de GDPR te voldoen.
De organisatie komt uit een land met een door de EU goedgekeurde privacywetgeving.	Deze organisatie moet aan privacywetgeving voldoen die in ieder geval door de EU als voldoende streng wordt beschouwd.
De organisatie bevindt niet in een overzees gebied van een EU-land.	De kans is groot dat overzeese gebieden alsnog delen van de privacywetgeving van het land waaraan deze verbonden is overneemt.

In totaal worden de privacyverklaringen van 120 organisaties geanalyseerd. Waarvan 40 organisaties die aan de GDPR moeten voldoen, 40 organisaties die niet aan de GDPR hoeven te voldoen maar wel onder strenge privacywetgeving vallen en 40 organisaties die niet aan enige vorm van strenge privacywetgeving hoeven te voldoen. Van iedere organisatie wordt zowel de meest recente privacyverklaring, als de verklaring van vlak voor de introductie van de GDPR geanalyseerd.

3.2.2 Verkrijging privacyverklaringen

Veel organisaties, ook degene die niet geraakt worden door de GDPR publiceren een privacyverklaring op de website van de organisatie. Deze verklaring is publiekelijk toegankelijk en kan ten aller tijden worden ingezien.

Het verkrijgen van oudere privacy verklaringen is lastiger. Sommige organisaties bewaren de oude privacyverklaring in een publiekelijk toegankelijk archief, dit zijn veelal grotere organisaties die geraakt worden door de GDPR. Bij kleinere organisaties, met name buiten Europa blijkt echter dat alleen de meest recente privacyverklaring is gepubliceerd. In dat geval zou een oudere versie van het privacy beleid bij de organisatie opgevraagd moeten worden. Omdat het niet aannemelijk is dat alle organisaties deze oudere versie willen, of kunnen aanleveren is de verwachting dat er hier een kleinere set wordt verkregen. Dit zal uiteindelijk gevolgen hebben op de betrouwbaarheid van het resultaat. Ten slotte kan een oude versie van het privacybeleid worden verkregen middels historische zoekmachines als The Wayback Machine van The Internet Archive. Personen kunnen een snapshot van een bepaalde webpagina maken en deze archiveren, hierdoor is het oude privacybeleid van veel organisaties ook nog inzichtelijk.

3.2.3 Kwantificatie privacyverklaringen

Uit onderzoek van Tikkinen-Pira, Rohunen & Markkula is gebleken dat GDPR de volgende grote veranderingen omvat die in bijlage B zijn beschreven (Tikkinen-Piri, Rohunen, & Markkula, 2018). De privacyverklaring wordt per organisatie getoetst op deze punten en kan per onderdeel een score van nul tot één toegekend krijgen. Hierbij wordt de volgende verdeling aangehouden:

Tabel 4: Kwantificatie privacyverklaring

Aantal punten	Verklaring
0	Dit onderdeel wordt niet benoemd in de privacyverklaring.
1	Dit onderdeel wordt benoemd in de privacyverklaring.

Er is hierbij voor gekozen om alleen na te gaan of een onderdeel in de privacyverklaring benoemd wordt en niet in hoeverre het onderdeel beschreven wordt. Dit omdat in het laatste geval, de beoordeling van de mate van beschrijving niet voldoende objectief is. Het beoordelingsformulier kan worden gevonden in bijlage C.

3.3 Gegevensanalyse

Allereerst worden alle privacyverklaringen geplaatst in een van de volgende zes categorieën:

1. Meest recente privacyverklaring – organisatie geraakt door GDPR.
2. Meest recente privacyverklaring – organisatie niet geraakt door een strenge privacywetgeving.
3. Meest recente privacyverklaring – organisatie geraakt door een andere voldoende strenge privacywetgeving.
4. Privacyverklaring van voor 24 mei 2016 - organisatie geraakt door GDPR.
5. Privacyverklaring van voor 24 mei 2016 - organisatie niet geraakt door een strenge privacywetgeving.
6. Privacyverklaring van voor 24 mei 2016 - organisatie geraakt door een andere voldoende strenge privacywetgeving.

Daarna wordt per privacyverklaring de totaalscore berekend en in een dataset geplaatst. Vervolgens wordt de analyse per hypothese iets anders uitgevoerd.

3.3.1 Hypothese 1: Effect wet- en regelgeving op privacybeleid

Om deze hypothese te toetsen wordt er een variantieanalyse (ANOVA) uitgevoerd met de eindscores van de privacyverklaringen uit 2019. De variantieanalyse is een geschikte toets om het verschil van een continue waarde in meerdere categorische groepen van verschillende entiteiten te bepalen (Field, 2013)

Allereerst wordt er een dataset gemaakt met alle totaalscores en de deelscores voor iedere organisatie binnen de volgende drie categorieën:

1. GDPR en 2019 (Voor organisaties die door de GDPR worden geraakt.)
2. Non-GDPR en 2019 (Voor organisaties die niet door strenge privacywetgeving worden geraakt.)
3. GDPR-alike en 2019 (Voor organisaties die door een andere vorm van strenge privacywetgeving worden geraakt.)

Vervolgens moet de dataset in SPSS voorbereid worden door de variabelen en datatypes aan te geven. Wanneer de dataset voorbereid is kan deze allereerst verkend worden met enkele exploratieve analyses. Hierna kan de ANOVA uitgevoerd worden. Na het uitvoeren van de toets worden de volgende zaken voor iedere combinatie categorieën gerapporteerd (Field, 2013):

- De toetsscore *(F)* en de vrijheidsgraad *(…)*
- De asymptotische significantie *(p)*
- De effectgrootte *(Omega-kwadraat (ω^2))*

Hierbij kan volgens Kirk de effectgrootte als volgt worden geïnterpreteerd (Kirk, 1996):

- 0,01 = klein

- 0,06 = middelmatig
- 0,14 = groot

Een variantieanalyse moet aan de volgende assumpties voldoen (UvA, 2014):

- Normaliteit
- Homogeniteit
- Onafhankelijkheid

Zelfs als deze assumpties geschonden worden is een variantieanalyse voldoende robuust om betrouwbaar te zijn, maar voor de zekerheid wordt er een Kruskal-Wallistoets uitgevoerd om de resultaten van de variantieanalyse te bevestigen.

Om vervolgens te toetsen of tussen de drie categorieën een verschil zit tussen de mate waarin de respectievelijke categorie invloed heeft op de kwaliteit van de privacyverklaring worden de volgende t-toetsen uitgevoerd:

- GDPR en niet GDPR-alike
- GDPR en GDPR-alike
- Niet GDPR-alike en GDPR-alike

Bij deze t-toets worden de volgende zaken gerapporteerd (Field, 2013):

- De toetsscore *T)* en de vrijheidsgraad *(…)*
- De asymptotische significantie *(p)*
- De effectgrootte *(d)*

De effectgrootte wordt voor de T-toets bepaald met Cohens d. Volgens Cohen dat de effectgrootte als volgt worden geïnterpreteerd (Cohen J. , 1992):

- 0.2 = klein
- 0.5 = middelmatig
- 0.8 = groot

Een T-toets moet aan een normaliteitsassumptie voldoen. Mocht de dataset hier niet aan voldoen, dan kan dezelfde toets nogmaals worden uitgevoerd met de niet-parametrische Mann-Whitney test. Vervolgens kunnen de resultaten vergeleken worden om na te gaan of deze overeen komen met de T-toets.

Een variantieanalyse of Kruskal-Wallistoets is niet geschikt om de afzonderlijke beoordelingscriteria van de drie verschillende categorieën met elkaar te kunnen vergelijken, omdat deze waarden categorisch zijn in plaats van continu. Om deze waarden met elkaar te kunnen vergelijken wordt er een Pearson chikwadraattoets uitgevoerd op iedere beoordelingscriterium voor de drie categorieën (Field, 2013). Na het uitvoeren van de toets worden de volgende zaken voor iedere combinatie categorieën gerapporteerd (Field, 2013):

- De toetsscore *(X^2)* en de vrijheidsgraad *(…)*
- De asymptotische significantie *(p)*
- De effectgrootte *(V)*

Bij voorkeur wordt de effectgrootte bij een Pearson chikwadraattoets uitgedrukt in een kansberekening, maar bij analyse van meer dan twee categorieën is dat geen geschikte methode. In

plaats daarvan wordt de effectgrootte uitgedrukt in Cramers V (Cohen J. , 1988). Volgens Cohen kunnen de uitkomsten van Cramers V als volgt gecategoriseerd worden:

Tabel 5: Effectgroottes Cramers V (Cohen J., 1988)

Vrijheidsgraad	Klein effect	Middelmatig effect	Groot effect
1	0,10	0,30	0,50
2	0,07	0,21	0,35
3	0,06	0,17	0,29
4	0,05	0,15	0,25
5	0,04	0,13	0,22

3.3.2 Hypothese 2: Effect verloop van tijd op privacybeleid

Om deze hypothese te toetsen wordt er een serie statistische toetsen uitgevoerd. Allereerst wordt middels een reeks gepaarde T-toetsen vastgesteld of het verloop van tijd tussen 2016 en 2019 een significante invloed heeft het gehad op de privacyverklaring van organisaties. Hierbij worden de volgende sets getoetst (Field, 2013):

- GDPR 2016 en GDPR 2019;
- Niet GDPR-alike 2016 en niet GDPR-alike 2019;
- GDPR-alike 2016 en GDPR-alike 2019;
- Alle organisaties 2016 en alle organisaties 2019.

Wanneer blijkt dat er inderdaad een verband bestaat tussen het verloop van tijd en de kwaliteit van de privacyverklaring, kan onderzocht worden of er een significant verband bestaat tussen de kwaliteitsverandering van privacyverklaringen en de privacywetgeving waar een organisatie onder valt. Dit wordt gedaan door twee nieuwe variabelen aan te maken:

- Totaalscore 2019 – Totaalscore 2016: Hiermee kan het absolute verschil tussen de twee categorieën duidelijk worden gemaakt.
- (Totaalscore 2019 – Totaalscore 2016)/ 2016: Hiermee wordt de relatieve verandering per privacyverklaring inzichtelijk.

Voor ieder van de twee bovenstaande variabelen wordt er eerst een variantieanalyse (ANOVA) uitgevoerd om vast te stellen of er een verband bestaat tussen de privacywetgeving of de absolute of relatieve kwaliteitsverandering van de privacyverklaringen. Vervolgens wordt er middels drie onafhankelijke T-toetsen nagegaan of dit verband bij enkele categorieën sterker zichtbaar is dan bij anderen. De volgende sets worden getoetst middels de T-toets:

- GDPR en niet GDPR-alike;
- GDPR en GDPR-alike;
- Niet GDPR-alike en GDPR-alike.

Mocht niet aan de normaliteitsassumptie van de T-toets worden voldaan, dan kunnen de resultaten uit deze toets geverifieerd worden met die van de niet-parametrische Wilcoxon signed-rank toets.

Ten slotte wordt met een regressieanalyse vastgesteld of er een modererend effect bestaat van de categorie op de absolute en relatieve verandering in kwaliteit van het privacybeleid. Hierbij worden de volgende zaken gerapporteerd (Field, 2013):

- De toetsscore (R^2)
- De *B*-waarde

- De standaardfout van *B*
- De standardized *β*
- De significantie (*p*)

3.4 Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

Binnen een degelijk uitgevoerd onderzoek is het belangrijk dat de validiteit en de betrouwbaarheid geborgd zijn (Saunders, Lewis, & Thornhill, 2016).

3.4.1 Validiteit

Een van de belangrijkste kwaliteitseisen van wetenschappelijk onderzoek is de validiteit (Gelderman, 2016). Validiteit bestaat onder andere uit de volgende vormen (Yin, 2013; Saunders, Lewis, & Thornhill, 2016):

- De constructvaliditeit;
- De interne validiteit;
- De externe validiteit.

Constructvaliditeit

Constructvaliditeit, of meetvaliditeit staat voor de mate waarin hetgeen dat onderzocht wordt, ook daadwerkelijk wordt gemeten (Gelderman, 2016). Het belangrijkste punt binnen dit onderzoek dat invloed heeft op de constructvaliditeit is de mate van substantiële implementatie van de privacywetgeving Ten eerste bestaat er geen duidelijke definitie van goed privacybeleid. Wel bestaan er vele adviezen, richtlijnen en wetten waaruit blijkt wat gedegen privacybeleid zou moeten omvatten. Om deze reden is er ook voor gekozen om de GDPR als leidraad te gebruiken omdat dit wereldwijd een van de strenge privacywetgevingen is (Justitia.nl, sd).

Een ander probleem is het feit dat de daadwerkelijke implementatie van privacywetgeving lastig meetbaar is. Zoals Smith, Dinev & Xu aankaarten is intentie niet per sé een garantie voor daadwerkelijke actie (Smith, Dinev, & Xu, 2011). Met name omdat organisaties juist vanwege institutionele- of legitimiteitsredenen baat hebben om de schijn van een substantieel privacybeleid hoog te houden, kan men zich afvragen of Fishbeins theorie van beredeneerde actie ook voor deze situatie opgaat (Fishbein & Ajzen, 1975). Omdat het hier een exploratief onderzoek betreft wordt dit gebrek geaccepteerd. De verschillen tussen de intentie die blijkt uit de privacyverklaring en de daadwerkelijke implementatie daarvan zouden in een vervolgonderzoek getoetst kunnen worden.

Interne validiteit

De interne validiteit staat voor de mate waarin de causaliteit tussen de onafhankelijke en afhankelijke variabele wordt aangetoond (Gelderman, 2016) (Saunders, Lewis, & Thornhill, 2016). Deze validiteit wordt tijdens de analyse van de onderzoeksresultaten geborgd door statistisch aan te tonen dat er wel of juist geen verschil zit tussen de verschillende categorieën van privacyverklaring.

Externe validiteit

Ten slotte staat de externe validiteit voor de generaliseerbaarheid van het onderzoek (Gelderman, 2016) (Saunders, Lewis, & Thornhill, 2016). Allereerst is ervoor gekozen om dit onderzoek te beperken tot de invloed van privacywetgeving op de privacyverklaringen van een specifieke selectie van organisaties. De resultaten van dit onderzoek kunnen dus niet zomaar toegepast worden op andere soorten wetgeving. Door een voldoende hoeveelheid en verscheidenheid aan te onderzoeken organisaties te selecteren wordt getracht om het onderzoek binnen het onderzoeksbereik zo generiek mogelijk te maken. Dit kan bijvoorbeeld worden gedaan door organisaties van zo

verschillend mogelijke groottes, sectoren of landen te selecteren. Hierbij moet wel opgemerkt worden dat ten behoeve van de uitvoerbaarheid van het onderzoek, het onderzoek zich beperkt tot organisaties die aan de in hoofdstuk 3.2.1 beschreven eisen voldoen. Dit kan een negatieve impact hebben op de externe validiteit van het onderzoek.

3.4.2 Betrouwbaarheid

Met betrouwbaarheid wordt de stabiliteit en repliceerbaarheid van de onderzoeksresultaten bedoeld (Gelderman, 2016; Saunders, Lewis, & Thornhill, 2016). De betrouwbaarheid van het onderzoek wordt geborgd door de privacyverklaringen te beoordelen middels een tweepuntsschaal waarin alleen wordt gecontroleerd of het criterium wel, of niet aanwezig is. De aanwezigheid van een criterium uit de privacywetgeving is objectief te meten en wordt niet snel beïnvloed door persoonlijke voorkeuren. Hierdoor is de kans groot dat andere onderzoekers met dezelfde onderzoeksmethode bij dezelfde organisatie ook tot dezelfde conclusies komen.

3.4.3 Ethiek

Tijdens dit onderzoek worden weinig, tot geen ethische aspecten geraakt. Alle benodigde onderzoeksgegevens worden via het internet verkregen uit openbare publicaties van de te onderzoeken organisaties, zonder hulp vanuit deze organisaties. Wanneer deze openbare privacyverklaringen persoonsgegevens bevatten, dan worden deze gegevens verwijderd alvorens de publicatie in het onderzoek wordt opgenomen. Het enige ethische aspect dat wel geraakt wordt, is het gebrek aan toestemming van de te onderzoeken organisaties (Saunders, Lewis, & Thornhill, 2016). Omdat het hier openbare publicaties van rechtspersonen betreft, is dit minpunt binnen dit specifieke onderzoek acceptabel.

4. Resultaten

Voor dit onderzoek zijn 238 verschillende privacy verklaringen beoordeeld van organisaties van verschillende grootte uit verschillende sectoren.

Tabel 6: Aantal verklaringen per groep

Categorie	Nieuw/ Oud	Aantal verklaringen	Percentage
GDPR	2019	40	16,6%
GDPR	2016	40	16,6%
GDPR-alike	2019	40	16,6%
GDPR-alike	2016	40	16,6%
Niet GDPR-alike	2019	40	16,6%
Niet GDPR-alike	2016	40 (38)	16,6%
Totaal		**240**	**100%**

Twee organisaties hadden voor 24 mei 2016 geen publiekelijk beschikbaar privacy statement. Deze ontbrekende verklaringen zijn wel meegenomen in het onderzoek maar hebben een score van 0 gekregen. Deze privacy verklaringen komen van organisaties uit de volgende landen:

Tabel 7: Aantal privacyverklaringen per land

Categorie	Jurisdictie	Aantal verklaringen	Percentage
GDPR	Nederland	78	32,5%
	Frankrijk	2	0,8%
GDPR-alike	Canada	40	16,7%
	Nieuw-Zeeland	40	16,7%
Niet GDPR-alike	India	22	9,2%
	Australië	18	7,5%
	Filipijnen	12	5%
	Singapore	12	5%
	Zuid-Afrika	8	3,3%
	Maleisië	6	2,5%
	Thailand	2	0,8%
Totaal		**240**	**100%**

Met name in de categorie niet GDPR-alike bleek het lastig om een gelijk verdeeld aantal geschikte organisaties te vinden die in 2016 over een geïndexeerde website beschikten waarop een privacy statement beschikbaar is.

Verder is gebleken dat van de 120 organisaties waarvan de privacy verklaringen zijn geanalyseerd, er 19 begin 2016 exact hetzelfde privacy statement gebruikten als in 2019. Hiervan kwamen elf verklaringen uit Canada, vier uit de Filipijnen en de overige uit India, Australië en Nieuw-Zeeland.

Tabel 8: Aantal onveranderde privacyverklaringen

Land	Aantal onveranderde verklaringen	% onveranderd ten opzichte van totaal geanalyseerd uit dat land
Canada	11	55,0%
Filipijnen	4	66,7%
India	2	18,2%
Australië	1	11,1%
Nieuw-Zeeland	1	5,0%

Ten slotte was het mogelijk om van 225 verklaringen het aantal woorden te tellen en bij 215 verklaringen het aantal karakters. Wanneer dit niet mogelijk was kwam dit doordat de privacyverklaring dusdanig gefragmenteerd was dat de woorden of karakters niet goed geteld konden worden, de tekst van het statement niet geselecteerd kon worden of doordat het statement in een pdf-formaat werd aangeleverd. In het laatste geval kon de pdf-reader enkel het aantal woorden tellen.

4.1 Hypothese 1: Effect wet- regelgeving op privacybeleid

Uit een eerste verkenning van de meest recente privacyverklaringen, valt op dat privacyverklaringen van organisaties die aan de GDPR moeten voldoen ongeveer 87% beter worden beoordeeld dan bij organisaties die aan een andere wetgeving moeten voldoen. De standaarddeviatie van de scores is voor alle groepen in absolute waarden vergelijkbaar, maar relatief gezien is deze voor verklaringen uit het GDPR-gebied 23% van het gemiddelde. Dit terwijl de standaarddeviatie voor de gebieden met een niet GDPR-alike en een GDPR-alike privacywetgeving respectievelijk 31% en 39% is. Dit laatste kan opvallend genoemd worden omdat verwacht zou worden dat een GPDR-alike privacywetgeving zorgt voor een betere consistentie tussen de verschillende privacyverklaringen.

Tabel 9: Beschrijvende statistieken hypothese 1

		N	Gemiddelde	Std-deviatie	Min.	Max.
Totaalscore 2019	GDPR	40	28.20	5.19	13	38
	Niet GDPR-alike	40	15.13	5.92	5	27
	GDPR-alike	40	15.73	6.13	4	30
	Totaal	120	19.68	8.32	4	38

Ditzelfde beeld is zichtbaar bij het merendeel van de afzonderlijke onderdelen van het beoordelingsformulier, waarbij de gemiddelde score bij organisaties die aan de GDPR moeten voldoen hoger beoordeeld zijn dan bij de andere twee categorieën. De standaarddeviatie bij organisaties die onder de categorie GDPR vallen is lager of vergelijkbaar ten opzichte van de andere categorieën (zie bijlage E.1). Wat verder opvalt is dat de relatieve standaarddeviatie bij enkele onderdelen zichtbaar hoger is dan bij anderen. Zo wijken privacyverklaringen bij onderdeel 7 “Automatische Besluitvorming” gemiddeld 239% af van het gemiddelde, terwijl dit bij het onderdeel 6 “Overdracht van Persoonsgegevens naar Derde Partijen” gemiddeld 56% is.

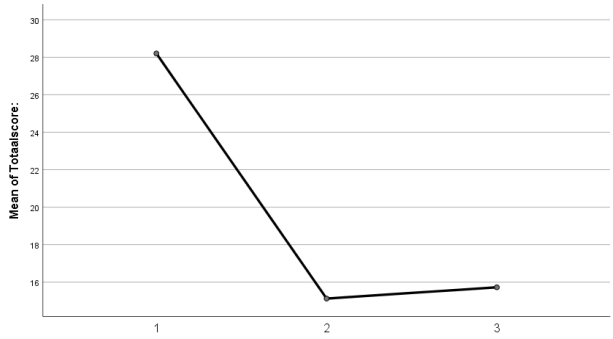
Tabel 10: Percentage voldaan aan criterium ten opzichte van het totaalaantal criteria per onderdeel. (Zie bijlage C voor beschrijving van onderdelen.)

Cat	Ond 1 (21)	Ond2 (9)	Ond3 (2)	Ond 4 (2)	Ond 5 (1)	Ond 6 (4)	Ond 7 (1)	Totaal (40)
GDPR	73,48%	81,11%	64,00%	80,00%	18,00%	52,00%	38,00%	53,00%
Niet GDPR-alike	41,10%	32,00%	60,00%	42,50%	5,00%	37,50%	3,00%	37,80%
GDPR alike	42,71%	38,33%	46,50%	47,50%	3,00%	33,75%	5,00%	39,33%

Verder blijkt dat er een aantal onderdelen in het beoordelingsformulier staan waarvan de criteria weinig voorkwamen in de privacyverklaringen van organisaties. Met name onderdeel 5 (Gedragsregels en Certificeringen) en onderdeel 7 (Automatische Besluitvorming) springen eruit omdat een kleine minderheid van de organisaties deze onderdelen opneemt in de privacyverklaring.

Wel is duidelijk dat organisaties die onder de categorie GDPR vallen in veel gevallen vaker aan een criterium per beoordelingsonderdeel voldoen dan organisaties die dat niet doen. Wat verder opvalt is dat organisaties die aan een GDPR-alike privacywetgeving moeten voldoen bij onderdeel 5 (Gedragsregels en Certificeringen) en onderdeel 6 (De Overdracht van Persoonsgegevens naar Derde Partijen) minder vaak aan de criteria voldoen dan organisaties die niet onderhevig zijn aan strenge privacywetten.

Wanneer wordt gekeken naar de homogeniteit van de dataset blijkt uit Levene's toets dat de assumptie van homogeniteit niet is geschonden (p = .168) Uit de Shapiro-Wilktest blijkt echter dat niet kan worden voldaan aan de normaliteitsassumptie (p = .297, zie bijlage D.1.1). Om deze reden worden de resultaten van de variantieanalyse geverifieerd middels een Kruskal-Wallistoets en Mann-Whitneytoets.



Figuur 3: Resultaat variantieanalyse totaalscore (1: GDPR, 2: not GDPR-alike, 3: GDPR-alike)

Uit het resultaat van de variantieanalyse blijkt dat de kwaliteit van privacyverklaringen in 2019 significant wordt beïnvloed door het gebied waarin de organisatie zich bevindt (F (2, 117) = 65.713, p < .001, ω^2 = .519). Dit effect is ook zichtbaar in de hiernaaststaande grafiek. Hierin is de volgende classificatie gebruikt:

1. GDPR
2. Not GDPR-alike
3. GDPR-alike

Wanneer wordt gekeken of er een significant verschil bestaat tussen de totaalscore en de categorie blijkt dat de categorie GDPR met de andere twee categorieën significant verschilt. Er is geen significant verschil tussen de categorieën "not GDPR-alike" en "GDPR-alike" aangetoond. Ook in de niet-parametrische toetsen komt hetzelfde beeld naar voren.

Tabel 11: Vergelijking totaalscore tussen categorieën

Categorieën	Testscore (t) en vrijheidsgraden	Significantie (p)	Effectgrootte (d)
GDPR en not GDPR-alike	10.51 (78)	< .001	2.35
GDPR en GDPR-alike	9.83 (78)	< .001	2.20
Not GDPR-alike en GDPR-alike	-0.46 (78)	.657	0.10

Uit de resultaten per onderdeel op het beoordelingsformulier blijkt er een significant verband te zijn tussen de drie categorieën en de deelscore voor ieder onderdeel, op het onderdeel "de veiligheid van persoonsgegevens" na. In nagenoeg alle gevallen lijkt dit verschil enkel zichtbaar tussen de categorie GDPR en de andere twee categorieën. Tussen de andere twee categorieën is bij geen enkel onderdeel een significant verschil gedetecteerd. Ook hier zijn de bovenstaande resultaten vergelijkbaar met de Kruskal-Wallistoets.

Tabel 12: Resultaten variantieanalyse per onderdeel.

Onderdeel	Teststatistiek: (F) & vrijheidsgraden	Significantie: (p)	Effectgrootte: (ω^2)
1: Transparantie	1172.87 (2, 117)	< .001	.503 (groot)
2: De rechten van de betrokkene	463.12 (2, 117)	< .001	.539 (groot)

3: De veiligheid van persoonsgegevens	2.72 (2, 117)	.085	.025 (klein)
4: De functionaris van gegevensbescherming	13.27 (2, 117)	.001	.098 (middel)
5: Gedragsregels en certificeringen	0.52 (2, 117)	.034	.040 (klein)
6: De overdracht van persoonsgegevens naar derde partijen	10.87 (2, 117)	.01	.093 (middel)
7: Automatische besluitvorming	3.05 (2, 117)	< .001	.184 (groot)

Wanneer wordt gekeken bij welk van de bovenstaande onderdelen met een significantie onder de 0.05 de drie verschillende categorieën van elkaar verschillen, blijkt dat in alle gevallen alleen de categorie GDPR te zijn. De overige categorieën blijken op geen enkel onderdeel van elkaar te verschillen (zie bijlage D.2).

Middels een Pearson chikwadraattoets is bepaald of de jurisdictie waarin een organisatie zich bevindt, invloed heeft op het wel of niet aanwezig zijn van een onderdeel in de privacyverklaring. Wanneer wordt gekeken naar de criteria per onderdeel, blijkt dat de jurisdictie waaronder een organisatie valt voor de meeste criteria een significant effect heeft op het al dan niet aanwezig zijn van dit onderdeel (zie bijlage D.2). Bij tien van de veertig onderdelen is juist geen significant effect geconstateerd. Bij alle criteria met een significant verschil tussen de drie categorieën, zijn alle onderdelen vaker bij organisaties in GDPR-gebied aanwezig dan dit het geval is bij de organisaties uit de andere gebieden. In 27,5% van de gevallen blijkt een onderdeel van het privacy statement significant vaker aanwezig te zijn bij organisaties in landen met een niet-GDPR alike privacywetgeving, dan bij landen waarbij de wetgeving volgens de EU wel lijkt op de GDPR. Daarnaast valt het op dat bij drie van de twaalf criteria die duiden op een substantiëlere implementatie van een ander criterium, minder dan 25% van de organisaties binnen iedere jurisdictie over een privacy statement beschikt dat hieraan voldoet. Slechts één criterium is met meer dan vijftien procentpunt aanwezig bij organisaties die aan een GDPR-alike privacywetgeving moeten voldoen in vergelijking met organisaties die aan een niet-GDPR alike wetgeving voldoen. Ten slotte is gebleken dat wanneer de categorieën niet GDPR-alike en GDPR-alike worden vergeleken, er slechts één criterium is met een significant verband tussen de jurisdictie en het al dan niet voldoen aan dit criterium. Bij de overige criteria was het verband tussen de categorieën niet GDPR-alike en GDPR-alike niet significant.

4.2 Hypothese 2: Effect verloop van tijd op privacybeleid

Wanneer privacyverklaringen uit 2019 en 2016 met elkaar worden vergeleken komt het volgende beeld naar voren:

Tabel 13: Vergelijking beoordelingen privacyverklaringen tussen 2019 en 2016

Jaar	Gemiddelde	Mediaan	Minimum	Maximum	Bereik	Standaarddeviatie
2019	19.68	20	4	38	34	8.32
2016	12.92	13	0	28	28	5.85

Hieruit valt op te merken dat wereldwijd gezien het gemiddelde privacy statement in 2019 53% beter wordt beoordeeld dan in 2016. Wel is de standaarddeviatie iets toegenomen, wat doet vermoeden dat het verschil in kwaliteit tussen de verschillende verklaringen iets is toegenomen ten opzichte van 2016.

Tabel 14: Vergelijking beoordelingen privacyverklaringen tussen 2019 en 2016 per categorie

Jaar	Wetgeving	Gemiddelde	Mediaan	Minimum	Maximum	Bereik	Standaarddeviatie
2019	GDPR	28.20	29	13	38	25	5.19
	Not GDPR-Alike	15.12	16	5	27	22	5.92
	GDPR-Alike	15.73	16	4	30	26	6.13
2016	GDPR	13.05	14	3	28	25	6.02
	Not GDPR-Alike	12.77	12	0	22	22	6.25
	GDPR-Alike	12.93	13	4	23	19	5.41

Wanneer er een laag dieper wordt gekeken vallen er een aantal zaken op. De geselecteerde privacy verklaringen werden in 2016 gemiddeld gezien nagenoeg gelijk beoordeeld. De standaarddeviatie ligt in 2016 voor alle groepen tussen de 5 en de 6, wat respectievelijk ongeveer 38,5% en 46,2% van het gemiddelde is. Uit de beoordelingen van geselecteerde verklaringen uit 2019 blijkt dat de gemiddelde beoordeling van verklaringen uit het GDPR-gebied met gemiddeld 15 punten (115,4%) is gestegen ten opzichte van 2016. De beoordeling van verklaringen uit het gebied met een niet GDPR-alike, is met 2 punten (15,4%) gestegen. In het geval van verklaringen uit het gebied dat een GDPR-alike wetgeving kent is dat 3 punten (23,1%). De standaarddeviatie van de scores is voor alle categorieën in absolute waarden nauwelijks gewijzigd, maar relatief gezien is deze in 2019 gedaald ten opzichte van 2016. Met name het verschil van de groep GDPR valt op, met een daling van 41,8% tot 18,4%.

Tabel 15: Vergelijking percentage voldaan aan criterium ten opzichte van het totaalaantal criteria per onderdeel tussen 2016 en 2019

Jaar	Cat	Ond 1 (21)	Ond2 (9)	Ond3 (2)	Ond 4 (2)	Ond 5 (1)	Ond 6 (4)	Ond 7 (1)	Totaal (40)
2019	GDPR	73,48%	81,11%	64,00%	80,00%	18,00%	52,00%	38,00%	53,00%
	Niet GDPR-alike	41,10%	32,00%	60,00%	42,50%	5,00%	37,50%	3,00%	37,80%
	GDPR alike	42,71%	38,33%	46,50%	47,50%	3,00%	33,75%	5,00%	39,33%
2016	GDPR	36,29%	38,56%	32,50%	12,50%	10,00%	23,25%	3,00%	32,63%
	Niet GDPR-Alike	35,10%	24,22%	51,50%	40,00%	10,00%	32,00%	0,00%	31,93%
	GDPR alike	35,24%	31,44%	33,50%	37,50%	0,00%	31,75%	0,00%	32,33%

Uit de resultaten is verder gebleken dat organisaties die aan de GDPR moeten voldoen, in veel gevallen aan meer beoordelingscriteria voldoen dan ten opzichte van 2016.

Wanneer er ook wordt gekeken naar de verschillende scores per jurisdictie lijkt het erop dat de gemiddelde score per land sterk kan verschillen, terwijl de standaarddeviatie tussen de 5 en 7 blijft. Dit verschil kan verklaard worden doordat ieder land buiten GDPR-gebied een eigen privacywetgeving heeft, die andere eisen stelt aan de manier waarop organisaties de privacy van klanten waarborgen. Hierbij moet ook opgemerkt worden dat de hoeveelheid privacyverklaringen per jurisdictie verschilt en er uit enkele landen een kleine hoeveelheid organisaties is geselecteerd.

Wanneer ten slotte wordt gekeken naar de gemiddelde totaalscore per land, blijkt dat met name de gemiddelde beoordeling van privacyverklaringen uit landen in GDPR-gebied en uit Zuid-Afrika sterk is

gestegen ten opzichte van 2016. De beoordeling van privacyverklaringen uit Canada en Nieuw-Zeeland (beiden met GDPR-alike wetgeving) zijn met respectievelijk 15,4% en 29,1% gestegen. De beoordeling van privacyverklaringen uit de Filipijnen en Maleisië zijn met respectievelijk 5,7% en 9,1% gestegen.

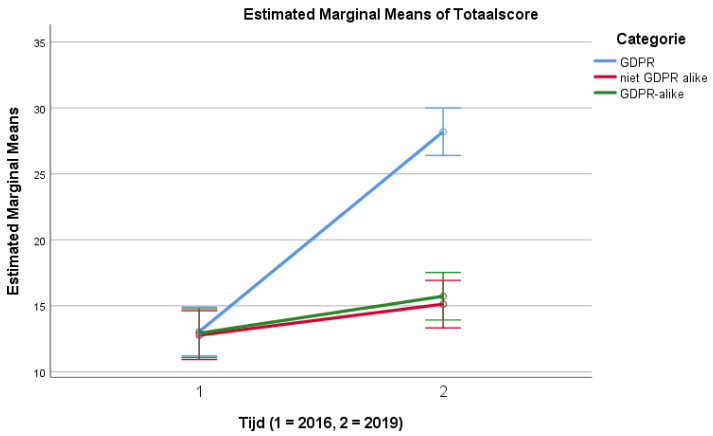
Uit de Shapiro-Wilktest blijkt wederom dat niet voor alle resultaten wordt voldaan aan de normaliteitsassumptie (zie bijlage E.1.1). Om deze reden worden de resultaten van de variantieanalyse geverifieerd middels niet parametrische toetsen.

In een serie gepaarde T-toetsen is nagegaan of de kwaliteit van de privacyverklaringen tussen 2016 en 2019 significant is gestegen. Hieruit is gebleken dat de kwaliteit voor zowel iedere categorie afzonderlijk als voor de hele dataset significant hoger ligt dan in 2016 het geval was. Met name het effect van tijd op de kwaliteit van privacyverklaringen bij organisaties die aan de GDPR moeten voldoen valt op. Wanneer gekeken wordt naar de t-scores per onderdeel van het beoordelingsformulier, blijkt dat voor de categorie GDPR alleen bij het onderdeel Gedragsregels en Certificeringen geen significant verschil tussen 2016 en 2019 is geconstateerd. Bij de andere twee categorieën is juist gebleken dat de onderdelen Transparantie, Rechten van de Betrokkenen zijn veranderd tussen de twee metingen. Bij de categorie niet GDPR-alike is dit ook het geval voor het onderdeel Veiligheid van Persoonsgegevens (zij bijlage E.1).

Tabel 16: Resultaten paired samples T-toets per categorie

Paar	Testscore (*t*) en vrijheidsgraad	Significantie (*p*)	Effectgrootte (*d*)
Complete set 2016 en Complete set 2019	-9.33 (119)	< .001	0.94
GDPR 2016 en GDPR 2019	-14.51 (39)	< .001	2.70
Niet GDPR-alike 2016 en Not GDPR-alike 2019	-4.09 (39)	< .001	0.39
GDPR-alike 2016 en GDPR alike 2019	-3.38 (39)	.002	0.48

Naar aanleiding van de bovenstaande resultaten is onderzocht of verbetering van kwaliteit van privacyverklaringen tussen 2016 en 2019 per categorie significant van elkaar verschilt. Uit het resultaat van de ANOVA blijkt dat de kwaliteit van privacyverklaringen tussen 2016 en 2019 voor iedere categorie significant verschilt (F (2, 115) = 75.08, p < .001, ω^2 = .55). Volgens de kwalificatie van Kirk is het effect van de wetgeving zeer groot (Kirk, 1996). Wanneer wordt gekeken naar de scores per onderdeel, wordt er wederom alleen bij het onderdeel Gedragsregels en Certificeringen geen significant verschil geconstateerd (zie bijlage E.2).



Figuur 4: Verschil gemiddelde totaalscores tussen 2016 (1) en 2019 (2) per categorie

Om vervolgens na te gaan of de verschillende categorieën hetzelfde effect hebben op de verbetering van kwaliteit, zijn drie verschillende onafhankelijke T-toetsen uitgevoerd:

- GDPR en not GDPR-alike
- GDPR en GDPR-alike

- Not GDPR-alike en GDPR alike

Hier zijn het volgende resultaat uit gekomen:

Tabel 17: Resultaten onafhankelijke T-test absolute verandering tussen 2016 en 2019

Categorieën	Testscore (*t*) en vrijheidsgraad	Significantie (*p*)	Effectgrootte (*d*)
GDPR en not GDPR-alike	10.92 (78)	< .001	2.40
GDPR en GDPR-alike	2.15 (78)	< .001	2.07
Niet GDPR-alike en GDPR-alike	3.20 (78)	.078	0.10

Hieruit blijkt dat er een significant verschil met een grote effectgrootte **is** tussen de absolute toename van kwaliteit in de privacyverklaringen van de categorie GDPR en de overige twee categorieën. Daarentegen is er geen significant verschil geconstateerd in kwaliteitstoename tussen de categorieën niet GDPR-alike en GDPR-alike. Hoewel statistisch niet significant, valt op dat de categorie niet GDPR-alike een groter effect had op de absolute verandering van de kwaliteit dan de categorie GDPR-alike.

Wanneer wordt gekeken naar de regressie tussen de absolute verandering in privacyverklaringen tussen 2016 en 2019 en de wetgeving waar de organisatie onder valt, zijn de volgende resultaten zichtbaar:

Tabel 18: Resultaten multivariate regressie absolute verandering wanneer onder invloed van non-GDPR alike en GDPR-alike wetgeving.

R^2 = .56	*B*	Standaardfout B	*Gestandaardiseerde β*	*p*
(Constante)	15.15	0.84		< .001
Niet GDPR-alike	-12.80	1.19	-.76	< .001
GDPR-alike	-12.35	1.19	-.76	< .001

Hieruit is gebleken dat de absolute verandering in kwaliteit bij organisaties die niet aan de GDPR hoeven te voldoen, significant lager is dan bij organisaties die hier wel aan moeten voldoen. In het geval van organisaties die aan een Not GDPR-alike wetgeving moet voldoen wordt verwacht dat de groei 12.80 punten lager ligt dan bij organisaties die aan de GDPR moeten voldoen. Bij organisaties die aan een GDPR-alike wetgeving moeten voldoen is dit verschil 12.35 punten lager.

Deze testen zijn ook herhaald met de relatieve veranderingen in kwaliteit in 2019 ten opzichte van 2016. Hieruit is gebleken dat er ook hierin een significant verband bestaat tussen de relatieve verandering in de privacyverklaring en de wetgeving waar de organisatie onder valt (F (2, 115) = 19,85, p < .001, ω^2 = .24).

Wanneer de losse categorieën worden vergeleken ontstaat het volgende beeld:

Tabel 19: Resultaten onafhankelijke T-test relatieve verandering tussen 2016 en 2019

Categorieën	Testscore (*t*) en vrijheidsgraad	Significantie (*p*)	Effectgrootte (*d*)
GDPR en not GDPR-alike	5.09 (76)	< .001	1.67
GDPR en GDPR-alike	4.35 (78)	< .001	0.97
Niet GDPR-alike en GDPR-alike	-0.93 (76)	.357	0.21

Ook wanneer wordt gekeken naar de relatieve verandering, blijkt er een significant verschil te bestaan tussen de categorie GDPR en de overige categorieën. Het verschil tussen de overige twee categorieën is wederom niet statistisch significant.

Wanneer wordt gekeken naar de regressie tussen de relatieve verandering in privacyverklaringen tussen 2016 en 2019 en de wetgeving waar de organisatie onder valt, zijn de volgende resultaten zichtbaar:

Tabel 20: Resultaten multivariate regressie relatieve verandering wanneer onder invloed van niet-GDPR alike en GDPR-alike wetgeving

R^2 = .26	*B*	Standaardfout *B*	*Gestandaardiseerde β*	Significantie (*p*)
(Constante)	1.85	0.20		< .001
Niet GDPR-alike	-1.63	0.29	-.52	< .001
GDPR-alike	-1.48	0.29	-.48	< .001

Hieruit blijkt dat het beeld dat ontstaat bij de absolute verandering, ook bij de relatieve verandering wederom naar voren komt.

5. Discussie, conclusies en aanbevelingen

Uit de verkennende beschrijvende statistieken voor beide hypothesen vallen een aantal zaken op. Ten eerste blijkt dat de beoordelingen van organisaties binnen iedere jurisdictie niet gelijk verdeeld zijn. Dit wordt mogelijk veroorzaakt door de relatief kleine hoeveelheid aan privacyverklaringen per categorie. Een tweede verklaring kan zijn dat er binnen de categorie niet GDPR-alike organisaties uit veel verschillende landen zijn geselecteerd die ieder een eigen privacywetgeving kennen. Dit verklaart echter niet waarom de beoordelingen van privacyverklaringen uit GDPR-gebied in 2019 niet normaal verdeeld waren, terwijl de privacyverklaringen uit Nieuw-Zeeland en Canada dit in datzelfde jaar wel waren.

Daarnaast is opgevallen dat een zeer klein deel van de organisaties heeft voldaan aan de criteria in de volgende onderdelen:

- 5: Gedragsregels en certificeringen;
- 7: Automatische besluitvorming.

Het is gebleken dat slechts een klein gedeelte van de organisaties voldoet aan bepaalde normen of certificeringseisen. De reden hierachter valt niet binnen de scope van dit onderzoek, maar het lijkt erop dat de bevindingen van Miyazaki en Krishnamurthy niet actief gebruikt worden door organisaties wanneer het een privacyverklaring betreft.

Daarnaast is gebleken dat organisaties nauwelijks communiceren of zij gebruik maken van automatische besluitvorming. Ditzelfde beeld komt ook naar voren bij het criterium “De verwerkingsverantwoordelijke geeft aan of er bijzondere persoonsgegevens worden verwerkt.” Een mogelijke verklaring hiervoor is dat organisaties alleen communiceren over deze zaken als de organisatie deze ook daadwerkelijk toepast. Dit is helaas minder transparant dan wanneer een organisatie ook concreet aangeeft dat bepaalde zaken die een grote impact hebben op de privacy van betrokkenen niet van toepassing zijn.

5.1 Discussie hypothese 1: Effect wet- regelgeving op privacybeleid

De eerste hypothese luidde als volgt: *Een organisatie die onderhevig is aan strenge privacy-gerelateerde wet- of regelgeving beschikt over een privacyverklaring van betere kwaliteit dan organisaties die niet aan strenge privacy-gerelateerde wet- en regelgeving moeten voldoen.*

Uit de onderzoeksresultaten viel direct op dat de gemiddelde beoordeling van privacybeleid bij organisaties uit GDPR-gebied met een score van 28 in 2019 hoger ligt dan bij de andere organisaties uit datzelfde jaar. Opvallend genoeg scoren organisaties uit gebieden met een GDPR-alike privacywetgeving niet veel beter dan organisaties die niet uit die gebieden komen (respectievelijk 15.73 en 15.13).

Uit de variantieanalyse is gebleken dat het de privacywetgeving waaraan een organisatie moet voldoen een significante invloed heeft op de kwaliteit van de privacyverklaring van die organisatie (F (2, 117) = 65.713, $p < .001$, $\omega^2 = .519$). Hierbij valt op dat met name organisaties die aan de GDPR moeten voldoen op het gebied van privacyverklaringen significant beter beoordeeld worden ten opzichte van de andere twee categorieën ($I\text{-}J = 13.075$, $p < .001$ en $I\text{-}J = 12.475$, $p < .001$). De privacyverklaringen van organisaties die moeten voldoen aan een GDPR-alike privacywetgeving, worden echter niet significant beter beoordeeld dan bij organisaties die aan een andere privacywetgeving moeten voldoen ($I\text{-}J = 0.600$, $p < .001$). Dit maakt het beantwoorden van de hypothese lastiger, omdat de verwachting zou zijn dat als de GDPR een positieve invloed zou hebben

op het privacybeleid van organisaties, andere gedegen privacywetgeving eenzelfde soort effect laat zien. Hoewel het niet binnen de scope van dit onderzoek past, kan dit mogelijk als volgt te verklaren zijn:

1. De criteria die de EU doet bepalen dat privacywetgeving van voldoende kwaliteit is zijn niet duidelijk te achterhalen uit publieke privacyverklaringen van organisaties en vallen daarmee buiten de scope van dit onderzoek. Denk hierbij aan interne instructies hoe er met persoonsgegevens moet worden omgegaan, of de manier waarop overheden persoonsgegevens mogen opvragen bij organisaties.
2. Tijdens het selecteren van organisaties is niet expliciet rekening gehouden met de grootte, de sector en de doelgroep van de organisatie. Hoewel er wel getracht was om in landen met GDPR-alike wetgeving en met name het GDPR-gebied een zo divers mogelijke set organisaties te selecteren, was dit wegens onbekendheid van de markt in het niet GDPR-alike gebied niet altijd mogelijk. Om deze reden bestaat 72,5% van de geselecteerde organisaties uit online retailers met een relatief hoge omzet. Hoewel deze organisaties niet aan de GDPR hoeven te voldoen, is het mogelijk dat deze organisaties gezien de grote hoeveelheden persoonsgegevens die zij verwerken ook een beter privacybeleid hanteren dan andere organisaties in dezelfde gebieden.
3. Er bestaat een andere variabele die invloed heeft op de kwaliteit van het privacybeleid dan wetgeving, die wel van toepassing is binnen de EU, maar niet daarbuiten.
4. De privacywetgeving in landen die volgens de EU een degelijke privacywetgeving zouden hebben, blijkt in de praktijk minder sterk dan verwacht.

Wanneer wordt gekeken naar het verband tussen de jurisdictie en de gemiddelde beoordeling per onderdeel valt op dat het privacybeleid van Europese organisaties op zes van de zeven onderdelen significant beter wordt beoordeeld dan in de andere gebieden. Het enige onderdeel waar dat niet zo is, is het onderdeel 3, “de Veiligheid van Persoonsgegevens” (p = .085). Dit onderdeel bestond uit twee criteria, waarbij er bij een criterium werd gekeken naar concrete voorbeelden van beveiligingsmaatregelen. Slechts 27 van de 120 privacyverklaringen bevatten concrete voorbeelden, die vrij gelijk waren verdeeld over de verschillende jurisdicties (zie bijlage E.2.3). Ook bij de losse onderdelen is in geen geval een significant verschil gedetecteerd tussen de categorie “niet GDPR-alike” en “GDPR-alike”.

Dit beeld blijft bestaan bij het vergelijken van de resultaten per jurisdictie per criterium. Bij 75% van de veertig criteria is er een significant verband geconstateerd tussen het aanwezig zijn van een bepaald onderdeel in de privacyverklaring en de jurisdictie. In slechts één geval, het niet rekenen van kosten om betrokkenen in staat te stellen om gebruik te maken van hun privacyrechten, is er een significant verschil geconstateerd tussen organisaties uit gebieden met een GDPR-alike privacybeleid en organisaties die moeten voldoen aan een niet GDPR-alike wetgeving (X^2 (1) = 0.24.757, p = < .001, V = .556). Hierbij was de kans zelfs hoger dat de organisatie geen kosten doorberekend wanneer deze is gevestigd in een land waar de privacywetgeving niet in orde is.

Het is echter duidelijk dat het wel of niet moeten voldoen aan de GDPR een grote invloed heeft op de kans of organisaties aan een bepaald criterium voldoen. Bij 50% van de criteria bleek dit verband groot, tot zeer groot te zijn. Bij twaalf van de vijftien criteria die duiden op een substantiële implementatie van de privacywetgeving, zoals concrete voorbeelden van maatregelen, bleek er een significant verband te zijn tussen de aanwezigheid van dit criterium en de jurisdictie. Het lijkt er dus op dat organisaties die aan de GDPR moeten voldoen, meer aandacht besteden aan de kwaliteit van de privacyverklaring dan organisaties buiten dit gebied.

5.2 Discussie hypothese 2: Effect verloop van tijd op privacybeleid

De tweede hypothese van dit onderzoek was de volgende: *De privacyverklaring van organisaties die onderhevig zijn geworden aan strengere privacy-gerelateerde wet- of regelgeving is na verloop van tijd privacyvriendelijker geworden dan organisaties die in dezelfde periode niet onderhevig zijn geworden aan strengere privacy-gerelateerde wet- of regelgeving.*

Uit de resultaten voor deze hypothese is gebleken dat de privacyverklaringen van alle onderzochte organisaties in 2019 significant beter worden beoordeeld dan in 2016 (T (119) = -9.33, p < .001, d = 0.94). Dit effect is het sterkst zichtbaar bij de categorie GDPR (T (39) = -14.51, p < .001, d = 2.70), maar ook significant aanwezig bij de overige twee categorieën. Wanneer wordt gekeken naar de afzonderlijke onderdelen binnen het beoordelingsformulier, blijkt dat organisaties binnen de categorie GDPR bij 86% van de onderdelen een significant hogere beoordeling krijgen, waarbij het onderdeel 5, “Gedragsregels en Certificeringen” de enige uitzondering is. Bij de categorie GDPR-alike was dit slechts 43%. Dit verschil wordt verklaard door het feit dat relatief veel van de onderzochte organisaties de privacyverklaring tussen 2016 en 2019 niet hebben bijgewerkt.

Vervolgens is onderzocht of de absolute verandering in privacyverklaringen tussen 2016 en 2019 wordt beïnvloed door de wetgeving waaraan een organisatie moet voldoen. Uit een ANOVA is gebleken dat de wetgeving ook een significante invloed heeft op de verandering in kwaliteit (F (2, 115) = 75.08, p < .001, ω^2 = .55). De omega-kwadraatscore duidt op een zeer groot effect. Ook qua relatieve verandering is alleen bij de categorie Gedragsregels en Certificeringen geen significante groei geconstateerd. Wanneer wordt gekeken naar de beschrijvende statistieken blijkt zelfs dat de gemiddelde beoordeling van organisaties die niet aan een GDPR-alike wetgeving moeten voldoen op dit onderdeel is gedaald van 0.1 in 2016, naar 0.05 in 2019. Mogelijke verklaringen voor deze daling zijn:

- Het privacybeleid van organisaties in landen met een niet-GDPR alike privacywetgeving is tussen 2016 en 2019 dusdanig gedaald dat deze organisaties niet meer voldoen aan de gestelde sectornormen, gedragsregels en certificeringen. Aangezien de gemiddelde kwaliteit van de privacyverklaring van deze organisaties in dezelfde periode wel is gestegen lijkt dit niet aannemelijk.
- Organisaties in landen met een niet-GDPR alike privacywetgeving zijn minder gevoelig geworden voor normatief isomorfisme en besteden daarom minder aandacht aan het voldoen van bepaalde sectornormen, gedragsregels en certificeringen.
- Organisaties in landen met een niet-GDPR alike privacywetgeving zijn vaker tot de conclusie gekomen dat hun klanten minder gevoelig zijn geworden voor organisaties die een bepaalde legitimiteit uitstralen middels sectornormen, gedragsregels en certificeringen.

Wanneer wordt gekeken naar de mate van absolute verandering tussen de verschillende soorten privacywetgeving, blijkt dat er een significant verschil zit tussen de verandering bij organisaties die aan de GDPR moeten voldoen en de andere organisaties. Het verschil in toename tussen organisaties die aan niet een aan GDPR-achtige wetgeving moeten voldoen en organisaties die dit wel doen, blijkt niet significant te zijn (T (78) = 3.20, p < .078, d = 0.10). Hierbij valt overigens op dat er geen significant verschil in de verandering tussen de categorie GDPR en de overige twee categorieën is geconstateerd tussen de beoordelingsonderdelen “Gedragsregels en Certificeringen” en “Veiligheid van de Persoonsgegevens”. Een exacte verklaring waarom de beoordeling van deze onderdelen weinig is veranderd en weinig verschilt tussen de categorieën valt echter niet binnen de scope van dit onderzoek.

Ten slotte is uit een regressieanalyse gebleken dat de privacywetgeving waaraan een organisatie zich moet houden een modererend effect heeft op de invloed van tijd op de kwaliteit van de privacyverklaring. Hierbij is opgevallen dat de kwaliteitsgroei die organisaties op het gebied van privacyverklaringen hebben doorgemaakt tussen 2016 en 2019 sterk afhankelijk is van de privacywetgeving waaraan moet worden voldaan. Hierbij is aangetoond dat het niet moeten voldoen aan de GDPR ervoor zorgt dat de privacyverklaring met ruim 12 punten lager wordt beoordeeld dan organisaties die wel aan de GDPR moeten voldoen. Hierdoor kan ook gezegd worden dat de privacywetgeving waaraan een organisatie moet voldoen, een modererend effect heeft op het verband tussen het verloop van tijd en de kwaliteit van de privacyverklaring.

Het bovenstaande beeld bij de absolute verandering is ook zichtbaar gebleken bij de relatieve verandering.

In het kort is dus gebleken dat de privacyverklaringen van alle organisaties tussen 2016 en 2019 inderdaad privacyvriendelijker zijn geworden. Daarnaast is aangetoond dat de privacywetgeving een modererend effect heeft op de mate waarin de privacyverklaring in deze periode is veranderd.

5.3 Conclusies

Tijdens dit onderzoek is nagegaan wat het effect van wetgeving is geweest op de kwaliteit van privacyverklaringen en of wereldwijde trends in de afgelopen jaren niet een vergelijkbaar effect hebben gehad. Allereerst kan worden gesteld dat er is aangetoond dat organisaties die moeten voldoen aan de GDPR een significant beter privacybeleid hebben dan organisaties die hier niet aan hoeven te voldoen. Uit dezelfde analyse is gebleken dat de kwaliteit van de privacyverklaringen van organisaties uit landen met een GDPR-alike privacywetgeving, niet significant beter zijn dan bij organisaties uit landen met een niet GDPR-alike wetgeving. Dit terwijl de privacywetgeving van die landen door de EU wel min of meer gelijkwaardig wordt geacht aan de GDPR.

Verder is bewezen dat de gemiddelde kwaliteit van privacyverklaringen tussen 2016 en 2019 significant is toegenomen. Organisaties die moeten voldoen aan de GDPR laten hierbij de grootste groei zien, terwijl er geen significant verschil is aangetoond tussen de organisaties uit landen met een GDPR-alike, of niet GDPR-alike wetgeving.

Al met al lijkt het zeer aannemelijk dat coërcitief isomorfisme middels wetgeving de verklaring is voor de verbetering van kwaliteit van privacyverklaringen. Er is ook gebleken dat de stijging van kwaliteit van privacyverklaringen bij organisaties in de EU samenvalt met de introductie van de GDPR. Hieruit kan geconcludeerd worden dat deze privacywetgeving in ieder geval binnen Nederland het gestelde doel heeft bereikt en daarmee ook dat wet- en regelgeving een effectieve methode is om het beleid van organisaties te veranderen. Daarnaast lijkt er sprake van een zekere vorm van mimetisch isomorfisme tussen organisaties. Dit omdat ook organisaties die aan een GDPR-alike privacywetgeving moeten voldoen, gemiddeld gezien een betere privacyverklaring hebben gekregen. Het is dus mogelijk dat de GDPR de aanleiding was dat organisaties buiten de EU deze wetgeving in hun privacybeleid nabootsen.

Hoewel het niet expliciet is getoetst in de hypothesen, lijkt het erop dat organisaties over het algemeen niet gevoelig zijn voor legitimiteitsaspecten. Slechts een klein deel van de organisaties heeft ervoor gekozen om het voldoen aan sectornormen, gedragsregels of certificaten in de privacyverklaring te communiceren.

Tijdens dit onderzoek is gebleken dat het verschil in kwaliteit van privacyverklaringen tussen organisaties die aan een GDPR-alike wetgeving moeten voldoen, niet significant verschillen of een andere groei hebben doorgemaakt dan organisaties die hier niet aan hoeven te voldoen. In een mogelijk vervolgonderzoek kan worden nagegaan hoe dit geringe verschil is ontstaan, of onderzoek naar de daadwerkelijke verschillen tussen GDPR-alike en niet GDPR-alike wetgeving ten opzichte van de verwachtingen die de EU over deze wetgeving heeft.

5.4 Reflectie

Zoals deels al eerder benoemd zijn er bij het voorbereiden van het onderzoek enkele keuzes gemaakt die bij nader inzien niet de meest geschikte bleken te zijn. Enkele van deze keuzes konden tijdig aangepast worden, maar in andere gevallen bleek het niet meer goed mogelijk om deze zaken achteraf aan te passen. Dit waren:

5.4.1 Selectie organisaties

Tijdens het onderzoek zijn er organisaties uit drie verschillende categorieën geselecteerd:

- Organisaties die onder de GDPR vallen;
- Organisaties die onder een GDPR-alike wetgeving vallen;
- Organisatie die niet onder een GDPR-alike wetgeving vallen.

Bij het selecteren van deze organisaties had er meer aandacht kunnen uitgaan naar het verdelen van organisaties over een gelijk aantal landen. Voor de categorie GDPR is dit een gering probleem omdat veel uitvoeringswetten voor een groot deel vergelijkbaar zijn, maar met name bij de organisaties met een niet GDPR-alike kan de kwaliteit van de lokale privacywetgeving van land tot land erg verschillen. Hierdoor kunnen de privacyverklaringen binnen dezelfde organisatie niet helemaal zuiver worden vergeleken. Een tweede aandachtspunt bij het selecteren van de organisaties is de sector, markt en grootte van deze organisatie. Deze factoren hebben mogelijk invloed op de kwaliteit van het privacybeleid. Om te voorkomen dat deze factoren invloed hebben op het resultaat, hadden er alleen organisaties geselecteerd moeten worden met een overeenkomstig profiel.

5.4.2 Opstellen beoordelingsformulier

Tijdens de analysefase van het onderzoek is het beoordelingsformulier meerdere malen aangepast. In de eerste instantie hield dit formulier geen rekening met criteria die duiden op een meer substantiële implementatie van een ander criterium. Achteraf zijn enkele van deze criteria toegevoegd, maar dit zorgde voor een grote hoeveelheid werk omdat een deel van de privacyverklaringen een tweede keer geanalyseerd moest worden. In andere gevallen bleek het achteraf te laat om de volgende extra criteria toe te voegen:

- Transparantie
    - De verwerkingsverantwoordelijke geeft aan waarom er bijzondere persoonsgegevens worden verwerkt.
    - De verwerkingsverantwoordelijke geeft aan wat de reden is om cookies te gebruiken.
    - De verwerkingsverantwoordelijke geeft een concrete tijdspanne af waarin er wordt gereageerd op privacy gerelateerde vragen of klachten.
- De veiligheid van persoonsgegevens
    - De verwerkingsverantwoordelijke geeft concrete voorbeelden van technische maatregelen om de persoonsgegevens te beschermen.

    - De verwerkingsverantwoordelijke geeft concrete voorbeelden van organisatorische maatregelen om de persoonsgegevens te beschermen.
    - De verwerkingsverantwoordelijke geeft concrete voorbeelden van fysieke maatregelen om de persoonsgegevens te beschermen.
- Gedragsregels en certificeringen
    - De verwerkingsverantwoordelijke legt uit wat de toegevoegde waarde van de genoemde sectornormen, gedragsregels of certificeringen is.
- De overdracht van persoonsgegevens naar derde partijen
    - De verwerkingsverantwoordelijke legt uit waarom er gegevens worden gedeeld met derde partijen.
- Automatische besluitvorming
    - De verwerkingsverantwoordelijke beschrijft globaal de werking van de automatische besluitvorming.
    - De verwerkingsverantwoordelijke legt uit waarom de automatische besluitvorming nodig is.

Deze wijzigingen zouden er waarschijnlijk voor zorgen dat het verschil tussen organisaties met een symbolisch privacybeleid en de organisatie met een substantieel privacybeleid duidelijker wordt. Daarnaast zorgt het toevoegen van extra vragen per onderdeel ervoor dat de resultaten van de statistische toetsen significanter van elkaar gaan verschillen.

Bij eventuele replicatie van dit onderzoek kunnen de bovenstaande suggesties verwerkt worden in de opzet van dat onderzoek.

6. Referenties

Aguilera, R. V., Rupp, D. E., Williams, C. A., & Ganapathi, J. (2007). Putting the S Back in Corporate Social Responsibility: A Multi-Level THeory of Social Change in Organizations. *Academy of Management Review*, 836-863.

Alpin. (2019, mei 30). *Major GDPR Fine Tracker – An Ongoing, Always-Up-To-Date List of Enforcement Actions*. Retrieved from Alpin: https://alpin.io/blog/gdpr-fines-list/

Argote, L., & Greve, H. R. (2007). A Behavioral Theory of the Firm - 40 Years and Counting: Introduction and Impact. *Organization Science*, 337-349.

Attili, V. S., Mathew, S. K., & Sugumaran, V. (2018). Understanding Information Privacy Assimilation in IT Organizations using Multi-site Case Studies. *Communications of the Association for Information Systems*, 66-94.

Autoriteit Persoonsgegevens. (2019, maart 14). Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2019). *Staatscourant*, pp. 1-15.

Autoriteit Persoonsgegevens. (n.d.). *Doorgifte binnen en buiten de EU*. Retrieved from Autoriteit Persoonsgegevens: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu#wat-houdt-het-eu-vs-privacyschild-in-5540

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 1017-1042.

Bell, J., & Waters, S. (2014). *Doing Your Research Project* . Maidenhead: Open University Press.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *Information Society*, 323-324.

Birnhack, M., & Elkin-Koren, N. (2011). Does Law Matter Online - Empirical Evidence on Privacy Law Compliance. *Michigan Telecommunications and Technology Law Review*, 337-384.

Bollen, L. (2019). Overzicht Academische Tijdschriften Binnen het IS/IM Vakgebied. Heerlen, Limburg, Nederland.

Burke, L., & Logsdon, J. M. (1996). How corporate social responsibility pays off. *Long Range Planning*, 495-502.

Carroll, A. B. (1998). The Four Faces of Corporate Citizenship. *Business and Society Review*, 1-7.

Christmann, P., & Taylor, G. (2006). Firm self-regulatie through internation certifiable standards: determinants of symbolic versus substantive implementation. *Journal of International Business Studies*, 863-878.

Clemens, B., & Douglas, T. J. (2006). Does coercion drive firms to adopt 'voluntary' green initiatives? Relationships amond coercion, superior firm resources, and voluntary green initiatives. *Journal of Business Research*, 483-491.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences.* New York: Lawrence Erblaum Associates.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, 155-159.

Cyert, R. M., & March, G. J. (1963). *A Behavioral Theory of the Firm.* Eaglewood Cliffs: Prentice Halls.

Davies, J. (2018, juni 3). GDPR: Implementing the regulations. (C. Laybats, Interviewer)

DiMaggio, P. J. (1988). Interest and agency in institutional theory. In L. G. Zucker, *Institutional patterns and organizations* (pp. 3-22). Cambridge: Ballinger.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizations. *American Sociological Review*, 147-160.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment. *Journal of Business Research*, 877-886.

Edelman, B. (2011). Adverse selection in online "trust" certifications and search results. *Electronic Commerce Research and Applications*, 17-25.

Europa Nu. (n.d.). *Landen en Gebieden Overzee (LGO)*. Retrieved from Europa Nu: https://www.europa-nu.nl/id/vh7dotcxc5zm/landen_en_gebieden_overzee_lgo

Fernando, S., & Lawrence, S. (2014). A theoretical framework for CSR practices: Integrating legitimacy theory, stakeholder theory and institutional theory. *Journal of Theoretical Accounting Research*, 149-178.

Ferrón-Vílchez, V. (2016). The dark side of ISO 14001: The symbolic environmental behavior. *European Research on Management and Business Economics*, 33-39.

Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics.* London: Sage.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading: Addison-Wesley.

Freeman, R. E., & Reed, D. L. (1983). Stockholders and Stakeholders: A New Perspective on Corporate Governance. *California Management Review*, 88-106.

Garber, J. (2018). GDPR - compliance nightmare or business opportunity. *Computer Fraud & Security*, 14-15.

Gelderman, C. J. (2016). Wetenschappelijk onderzoek en de afstudeerscriptie. In C. J. Gelderman, *Methoden en technieken van onderzoek: Reader 1* (pp. 8-17). Heerlen: Open Universiteit.

Greenwood, R., & Meyer, R. E. (2008). Influencing Ideas: A celebration of DiMaggio and Powell (1983). *Journal of Management Inquiry*, 258-264.

Iatridis, K., & Kesidou, E. (2018). What drives substantive versus symbolic implementation of ISO14001 in a time of economic crisis? Insights from Greek manufacturing companies. *Journal of Business Ethics*, 859-877.

Jankowicz, A. D. (2005). *Business Research Projects.* London: Thomson Learning.

Justitia.nl. (n.d.). *Privacy - bescherming persoonsgegevens*. Retrieved from Justitia.nl: https://www.justitia.nl/privacy/

Kirk, R. E. (1996). Practical Significance: A Concept Whose Time Has Come. *Educational and Psychological Measurement*, 746-759.

Lannelongue, G., Gonzalez-Benito, O., & Gonzalez-Benito, J. (2013). Environmental motivations: The pathway to complete environmental management. *Journal of Business Ethics*, 1-13.

Leupen, J., & Piersma, J. (2018, mei 25). *Onrust bij privacywaakhond Autoriteit Persoonsgegevens*. Retrieved from Het Financieele Dagblad: https://fd.nl/economie-politiek/1254871/onrust-bij-privacywaakhond-autoriteit-persoonsgegevens

Maack, M. M. (2018, december 27). *GDPR's impact was too soft in 2018, but next year will be different*. Retrieved from The Next Web: https://thenextweb.com/eu/2018/12/27/gdprs-impact-was-too-soft-in-2018-but-next-year-will-be-different/

Maack, M. M. (2019, maart 14). *The Netherlands premieres the first GDPR fining policy in the EU*. Retrieved from The Next Web: https://thenextweb.com/eu/2019/03/14/the-netherlands-premieres-the-first-gdpr-fining-policy-in-the-eu/

MacMillan, K. (2019). Struggling with the GDPR. *Computer Fraud & Security*, 20.

Magali, Sarfatti, & Larson. (1977). *The Rise of Proffessionalism: a Sociological Analysis.* Los Angeles: University of California Press.

Mebius, D. (2018, mei 25). *Privacywaakhond heeft te weinig handhavers voor kleine bedrijven; vooral controle overheid en zorg*. Retrieved from De Volkskrant: https://www.volkskrant.nl/nieuws-achtergrond/privacywaakhond-heeft-te-weinig-handhavers-voor-kleine-bedrijven-vooral-controle-overheid-en-zorg~b81129ed/

Meyer, J. W., & Rowan, B. (1991). Institutionalized organizations: Formal structure as myth and ceremony. In W. W. Powell, & P. J. DiMaggio, *The new institutionalism in organizational analysis* (pp. 41-61). Chicago: University of Chicago Press.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science*, 35-57.

Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *The Journal of Consumer Affairs*, 28-49.

MKB-Servicedesk. (2018, mei 2). *Aandacht MKB voor AVG verbeterd ondanks slechte voorlichting door overheid*. Retrieved from MKB Servicedesk: https://www.mkbservicedesk.nl/11226/aandacht-mkb-voor-avg-verbeterd-ondanks.htm

Parsons, T. (1960). *Structure and Process in Modern Societies.* Glencoe: The Free Press.

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS Quarterly*, 977-988.

Perez-Batres, L. A., Doh, J. P., Miller, V. V., & Pisani, M. J. (2012). Stakeholder Pressures as Determinants of CSR Strategic Choice: Why do Firms Choose Symbolic Versus Substantive Self-Regulatory Codes of Conduct? *Journal of Business Ethics*, 157-172.

Perry, R. (2019). GDPR - project or permanent reality? *Computer Fraud & Security*, 9-11.

Pollach, I. (2011). Online privacy as a corporate social responsibility: an emprical study. *Business Ethics: An European Review*, 88-102.

Rijksoverheid. (2018, juni 6). *Vragen van het lid Omtzigt (CDA) aan de staatssecretaris van Financiën over de Algemene verordening gegevensbescherming (AVG) en de Belastingdienst.* Retrieved from Rijksoverheid: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/06/05/antwoorden-op-vragen-over-de-avg-en-de-belastingdienst/antwoorden-op-vragen-over-de-avg-en-de-belastingdienst.pdf

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students.* Harlow: Pearson.

Schermer, B. W., Hagenauw, D., & Falot, N. (2018). *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene Verordening gegevensbescherming.* Den Haag: Ministerie van Veiligheid en Justitie.

Scott, R. W. (1987). The Adolescence of Institutional Theory. *Administrative Science Quarterly*, 493-511.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 989-1015.

Spataru-Negura, L.-C., & Lazar, C. (2018). Lifting the Veil of the GDPR tot Data Subjects. *Challenges of he Knowledge Society*, 658-667.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, 459-468.

Suchman, M. C. (1995). Managing Legitimacy: Strategic and Institutional Approaches. *Academy of Management*, 571-610.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 134-153.

UvA. (2014, juli 8). *One-way ANOVA - Methodologiewinkel*. Retrieved from UvA Wiki Methodologiewinkel: https://wiki.uva.nl/methodologiewinkel/index.php/One-way_ANOVA

Wallace, M., & Wray, A. (2011). *Critical Reading and Writing for Postgraduates.* London: Sage.

Westin, A. F. (1967). *Privacy And Freedom.* New York: Atheneum.

Yin, R. K. (2013). *Case Study Research.* London: Sage.

Yousafzai, S. Y., Foxall, G. R., & Pallister, J. G. (2010). Explaining Internet Banking Behavior: Theory of Reasoned Action, Theory of Planned Behavior, or Technology Acceptance Model? *Journal of Applied Social Psychology*, 1172-1202 .

Zailani, S. H., Eltayeb, K. T., Hsu, C.-C., & Tan, K. C. (2012). The impact of external institutional drivers and internal strategy on environmental performance. *International Journal of Operations & Production Management*, 722-745.

7. Overzicht afbeeldingen en tabellen

A. Zoekstrategie voor bouwblokmethode

Tijdens de literatuurstudie wordt er gezocht naar informatie over de volgende onderwerpen:

1. Hoe kan beleid als substantieel of symbolisch geclassificeerd worden?
2. Welke wetenschappelijke theorieën kunnen verklaren waarom organisaties ervoor kiezen om beleid te implementeren?
3. Welke wetenschappelijke kennis bestaat er op het gebied van privacy?
4. Wat is de General Data Protection Regulation?
5. Welke wetenschappelijke kennis bestaat er over de koppeling van wetenschappelijke theorieën en de implementatie van privacybeleid?

A.1 Zoekparameters

Volgens Bell en Waters is het verstandig om per deelvraag eerst na te denken over de zoekparameters te definiëren (Bell & Waters, 2014). Dit zijn:

- De taal waarin de publicatie is geschreven;
- Het vakgebied waarop het onderwerp is gericht;
- De sector waarop het onderwerp is gericht;
- De geografische locatie waarop de publicatie zich baseert;
- De maximale publicatiedatum;
- Het soort publicatie.

A.1.1 Hoe kan beleid als substantieel of symbolisch geclassificeerd worden?

Onderwerp	Keuze	Motivatie
Taal	Engels, Nederlands	De meeste internationale publicaties zullen in het Engels geschreven worden.
Vakgebied	-	Managementwetenschappen
Sector	-	Niet van toepassing, deze vraag richt zich niet op een bepaalde sector.
Locatie	Wereldwijd	Het verschil tussen volledig of symbolische naleving van wet- en regelgeving is een wereldwijd onderzocht probleem.
Maximale publicatiedatum	1 januari 2004	Deze vraag raakt niet per definitie een recent probleem dat aan veel verandering onderhevig is. Het is dan ook acceptabel om een zoekperiode van 15 jaar te gebruiken.
Soort publicatie	(Peer-reviewed) journal	Volgens Saunders, Lewis en Thornhill zijn journals het meest geschikt om een antwoord te krijgen op een wetenschappelijk vraagstuk (Saunders, Lewis, & Thornhill, 2016).

A.1.2 Welke wetenschappelijke theorieën kunnen verklaren waarom organisaties ervoor kiezen om beleid te implementeren?

Onderwerp	Keuze	Motivatie
Taal	Engels, Nederlands	De meeste internationale publicaties zullen in het Engels geschreven worden.
Vakgebied	-	Managementwetenschappen
Sector	-	Niet van toepassing, deze vraag richt zich niet op een bepaalde sector.
Locatie	Wereldwijd	De implementatie van beleid is een wereldwijd onderzocht probleem.

Maximale publicatiedatum	1 januari 2004	Deze vraag raakt niet per definitie een recent probleem dat aan veel verandering onderhevig is. Het is dan ook acceptabel om een zoekperiode van 15 jaar te gebruiken.
Soort publicatie	(Peer-reviewed) journal	Volgens Saunders, Lewis en Thornhill zijn journals het meest geschikt om een antwoord te krijgen op een wetenschappelijk vraagstuk (Saunders, Lewis, & Thornhill, 2016).

A.1.3 Welke wetenschappelijke kennis bestaat er op het gebied van privacy?

Onderwerp	Keuze	Motivatie
Taal	Engels, Nederlands	De meeste internationale publicaties zullen in het Engels geschreven worden.
Vakgebied	-	Managementwetenschappen/ Informatiewetenschappen
Sector	-	Niet van toepassing, deze vraag richt zich niet op een bepaalde sector.
Locatie	Wereldwijd	Privacy is een wereldwijd onderzocht probleem
Maximale publicatiedatum	1 januari 2004	Deze vraag raakt niet per definitie een recent probleem dat aan veel verandering onderhevig is. Het is dan ook acceptabel om een zoekperiode van 15 jaar te gebruiken.
Soort publicatie	(Peer-reviewed) journal	Volgens Saunders, Lewis en Thornhill zijn journals het meest geschikt om een antwoord te krijgen op een wetenschappelijk vraagstuk (Saunders, Lewis, & Thornhill, 2016).

A.1.4 Wat is de General Data Protection Regulation?

Onderwerp	Keuze	Motivatie
Taal	Nederlands, Engels	In principe worden Nederlandstalige bronnen verwacht omdat de vraag zich richt op organisaties die in Nederland actief zijn. Het zou kunnen dat enkele literatuurstukken gericht op niet-Nederlandse organisaties in het Engels zijn geschreven.
Vakgebied	-	Rechtswetenschappen
Sector	-	Niet van toepassing, deze vraag richt zich niet op een bepaalde sector.
Locatie	Nederland, Europa	In principe wordt er gezocht naar artikelen die zich richten op de Nederlandse wet- en regelgeving. Omdat het Europees recht ook van toepassing is in Nederland kan er ook gezocht worden naar bronnen die zich richten op de Europese Unie (EU).
Maximale publicatiedatum	1 januari 2012	Dit is de datum waarop het wetsvoorstel van de huidige General Data Protection Regulation (GDPR) is ingediend. Eerdere publicaties kunnen interessant zijn, maar hier wordt niet expliciet op gezocht.
Soort publicatie	Wettekst, Vakliteratuur, (Peer-reviewed) journal	Er wordt verwacht dat de meeste informatie met betrekking tot dit onderwerp is gepubliceerd in wetteksten en vakliteratuur.

A.1.5 Welke wetenschappelijke kennis bestaat er over de koppeling van wetenschappelijke theorieën en de implementatie van privacybeleid?

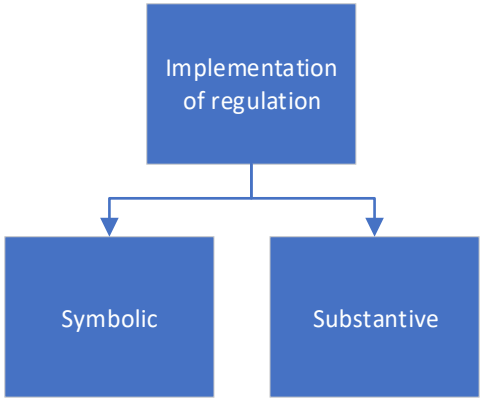
Onderwerp	Keuze	Motivatie
Taal	Engels, Nederlands	De meeste internationale publicaties zullen in het Engels geschreven worden.
Vakgebied	-	Managementwetenschappen/ Informatiewetenschappen
Sector	-	Niet van toepassing, deze vraag richt zich niet op een bepaalde sector.
Locatie	Wereldwijd	Dit is een wereldwijd onderzocht probleem.
Maximale publicatiedatum	1 januari 2004	Deze vraag raakt niet per definitie een recent probleem dat aan veel verandering onderhevig is. Het is dan ook acceptabel om een zoekperiode van 15 jaar te gebruiken.

Soort publicatie	(Peer-reviewed) journal	Volgens Saunders, Lewis en Thornhill zijn journals het meest geschikt om een antwoord te krijgen op een wetenschappelijk vraagstuk (Saunders, Lewis, & Thornhill, 2016).

A.1.6 Zoeksleutels

Een van de belangrijkste onderdelen van het voorbereiden van een literatuuronderzoek is het definiëren van de zoeksleutels. (Bell & Waters, 2014) Een hulpmiddel om per onderzoeksvraag de zoeksleutels te definiëren is het gebruik van een *relevance tree* (Jankowicz, 2005). Dit hulpmiddel helpt volgens Jankowicz bij het nemen van beslissingen met betrekking tot welke zoeksleutels relevant zijn voor de onderzoeksvraag en welke onderwerpen het meest belangrijk zijn om een onderzoeksvraag te kunnen beantwoorden.

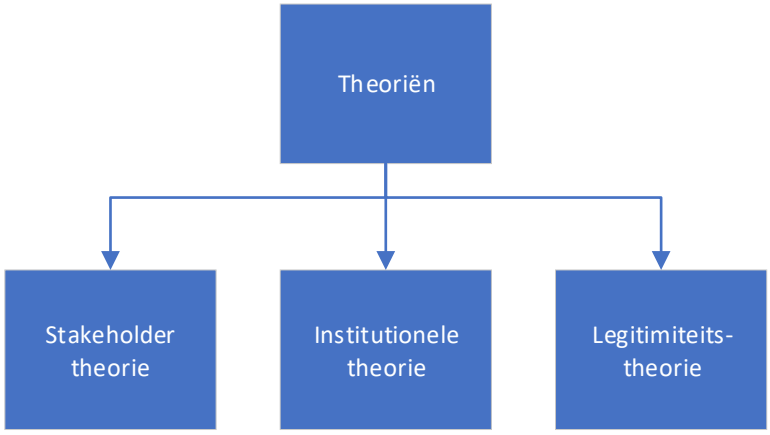
A.1.6.1 Hoe kan beleid als substantieel of symbolisch geclassificeerd worden?



Zoekopdrachten

Substant* OR Symbolic AND implementation

A.1.6.2 Welke wetenschappelijke theorieën kunnen verklaren waarom organisaties ervoor kiezen om beleid te implementeren?



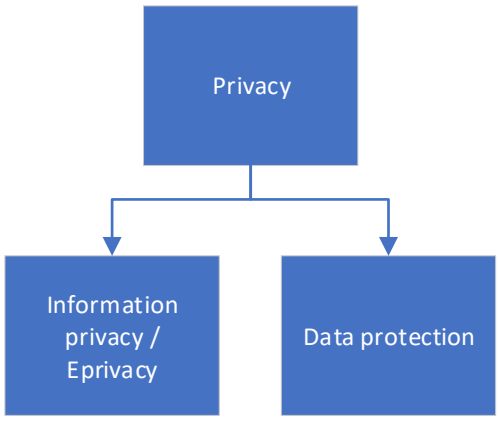
Zoekopdrachten

Stakeholder*

Instution* OR Transaction

Legitimacy*

A.1.6.3 Welke wetenschappelijke kennis bestaat er op het gebied van privacy?



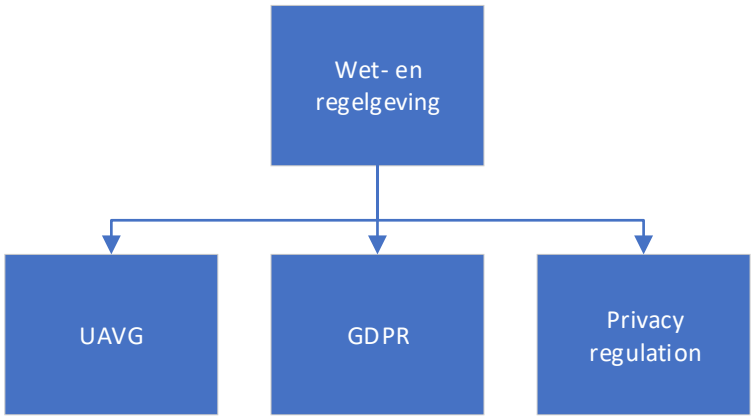
Zoekopdrachten

Privacy

***privacy**

Data protection

A.1.6.4 Wat is de General Data Protection Regulation?



Zoekopdrachten

AVG

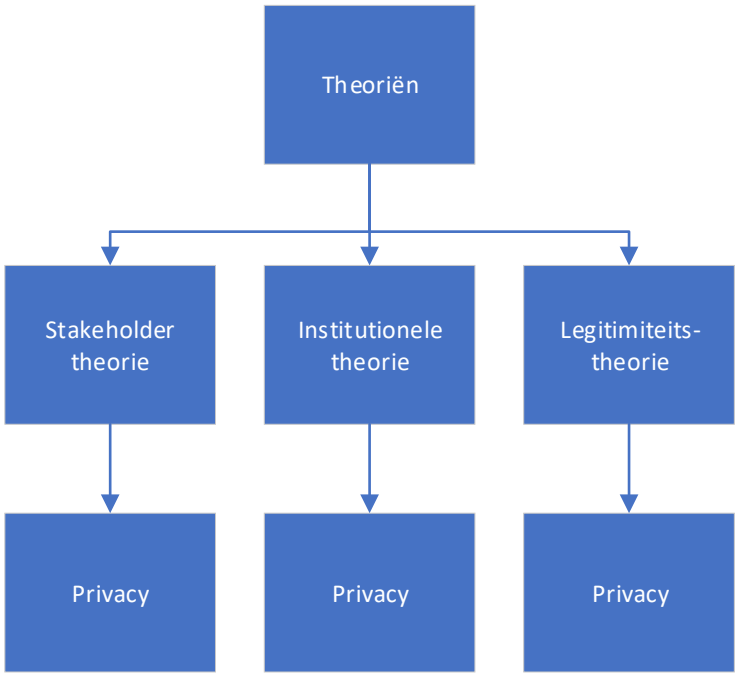
***AVG**

GDPR

***privacy OR Data protection AND Regulation**

Cookiewet

A.1.2.5 Welke wetenschappelijke kennis bestaat er over de koppeling van wetenschappelijke theorieën en de implementatie van privacybeleid?



Zoekopdrachten

Stakeholder* AND *Privacy

Institution* AND Privacy OR Transaction AND Privacy

Legitimacy* AND *Privacy

A.2 Databases en zoekmachines

Om vraag 4 te kunnen beantwoorden zijn er met name specifieke wetteksten nodig die via een standaard zoekmachine als Startpage kunnen worden verkregen. Voor de overige vragen kan de academische zoekmachine EBSCO Academic Search Elite gebruikt worden. Deze zoekmachine biedt toegang tot veel volledig inzichtelijke academische bronnen op het gebied van managementwetenschappen.

A.3 Overige criteria

Voor vraag 4 gaat de voorkeur uit naar primaire bronnen, zoals wetteksten of beschrijvingen van regelgeving. Waar nodig kan ook worden gezocht naar secundaire bronnen die deze wetteksten verduidelijken. Voor dit laatste gaat de voorkeur uit naar bronnen die door de wetgever, zoals de Europese Unie of de Rijksoverheid zijn geschreven.

Voor de overige vragen gaat de voorkeur uit naar wetenschappelijke artikelen die zijn gepubliceerd in een van de volgende zeer goed aangeschreven peer-reviewed journals (Bollen, 2019):

- MIS Quarterly;
- Information Systems Research;

- Journal of Management Information Systems;
- Information & Management;
- European Journal of Information Systems;
- Journal of the Association for Information Systems;
- Harvard Business Review;
- MISQ Executive;
- Communications of the ACM;
- California Management Review;
- MIT Sloan Management Review.

Wanneer het nodig is om extra diepgang te verkrijgen kan er ook voor gekozen worden om kleine stukken van andere, doch degelijke journals te gebruiken.

B. Verschillen tussen General Data Protection Regulation en Data Protection Directive 95/46/EC

Hieronder zijn de belangrijkste verschillen van de General Data Protection Regulation (GDPR) ten opzichte van de Data Protection Directive 95/46/EC (DIR95) opgenomen (Tikkinen-Piri, Rohunen, & Markkula, 2018) (Schermer, Hagenauw, & Falot, 2018).

Algemene bepalingen en principes

- Het bereik van de wetgeving is vergroot tot alle organisaties binnen de EU, of alle organisaties die persoonsgegevens van EU-ingezetenen verwerken;
- Er zijn een aantal nieuwe termen geïntroduceerd, zoals pseudonimiseren, inbreuk in verband met persoonsgegevens en genetische-, biometrische-, of gezondheidsdata;
- Nieuwe principes, zoals het transparant verwerken van persoonsgegevens, eindverantwoordelijkheid en verwerkingen die geen identificatie behoeven;
- Verduidelijking van bestaande principes, zoals data minimalisatie en de manier waarop toestemming voor verwerking mag worden verkregen;
- Het aanscherpen van eisen aan de toestemming om persoonsgegevens van personen jonger dan 16 jaar te verwerken.

Transparantie

- Verwerkingsverantwoordelijken moeten transparante en duidelijke informatie verschaffen over de verwerking van de persoonsgegevens van individuen;
- Verwerkingsverantwoordelijken moeten personen in staat stellen om gebruik te maken van hun door de GDPR gedefinieerde rechten;
- Verwerkingsverantwoordelijken moeten tijdig reageren op GDPR gerelateerde vragen en verzoeken van personen.

Informatie over en toegang tot de persoonsgegevens

- Verwerkingsverantwoordelijken moeten voorafgaand aan de dataverwerking personen informeren over de verwerkingsverantwoordelijke, de rechten van de persoon en naar welke andere landen de data verzonden kan worden;
- Wanneer de data van een persoon verwerkt wordt, heeft deze het recht om hier nogmaals geïnformeerd te worden en dient deze wederom op zijn of haar GDPR-gerelateerde rechten gewezen te worden.

Rectificatie, verwijdering en overdraagbaarheid

- Personen hebben het recht om de eigen persoonsgegevens te rectificeren, te laten wissen of de toegang tot deze gegevens te beperken;
- Personen hebben het recht om data te verplaatsen van het ene systeem naar een andere.

Bezwaar maken tegen geautomatiseerde individuele besluitvorming

- Personen mogen bezwaar maken tegen geautomatiseerde individuele besluitvorming. De verwerkingsverantwoordelijke moet aantoonbaar maken waarom de noodzaak tot deze besluitvorming opweegt tegenover de belangen van de betrokkene;

- Personen mogen alleen onderworpen worden aan geautomatiseerde individuele besluitvorming wanneer deze hier expliciet mee akkoord gaan.

Algemene verplichtingen voor verwerkingsverantwoordelijken

- Verwerkingsverantwoordelijken moeten de verwerking van persoonsgegevens bijhouden en registreren;
- De verplichtingen van verwerkingsverantwoordelijken in een situatie waarin meerdere verwerkingsverantwoordelijken samenwerken is aangescherpt;
- Verwerkingsverantwoordelijken moeten het *privacy by design* principe in hun processen en structuren toepassen.

De veiligheid van persoonsgegevens

- De manier waarop verplichtingen van gegevensverwerkers moet worden toegepast is verder verduidelijkt;
- Verwerkingsverantwoordelijken moeten nu datalekken melden bij de toezichthouder. In Nederland is dit de Autoriteit Persoonsgegevens (Schermer, Hagenauw, & Falot, 2018).
- Gegevensverwerkers moeten datalekken nu melden bij de verwerkingsverantwoordelijke.

De functionaris voor gegevensbescherming

- De verwerkingsverantwoordelijke moet nu een functionaris voor gegevensbescherming (ook wel data protection officer of DPO) aanwijzen wanneer de organisatie een overheidsorgaan is, de organisaties persoonsgegevens verwerkt die vanwege de schaal of doeleinden stelselmatige controle vereist, of wanneer de organisatie bijzondere categorieën persoonsgegevens verwerkt (Schermer, Hagenauw, & Falot, 2018).

Gedragsregels en certificeringen

- Gedragsregels kunnen sneller opgesteld worden door de toezichthouder;
- De introductie van nieuwe manieren om compliance met de GDPR aan te tonen, zoals certificaten en keurmerken.

De overdracht van persoonsgegevens naar andere landen of internationale organisaties.

- De voorwaarden om persoonsgegevens naar andere landen te mogen overdragen zijn verder aangescherpt.

Klachten, aansprakelijkheid en sancties

- Wanneer een persoon het idee heeft dat zijn of haar GDPR-gerelateerde rechten niet worden gehonoreerd, dan kan deze een klacht indienen bij de toezichthouder;
- Zowel de verwerkingsverantwoordelijke als de verwerker zijn nu verantwoordelijk voor de inbreuk op GDPR-gerelateerde rechten;
- Toezichthouders mogen boetes opleggen aan organisaties die inbreuk maken op GDPR-gerelateerde rechten.

C. Beoordeling privacyverklaring

Het onderstaande ontwerp is gebaseerd op de analyse van de GDPR door Tikkinen-Pira, Rohunen & Markkula. Deze analyse wordt ook beschreven in bijlage B (Tikkinen-Piri, Rohunen, & Markkula, 2018). In dit formulier staan enkele criteria die een aanvulling zijn op het voorafgaande criterium. Deze criteria zijn in het onderstaande formulier geel gearceerd.

Het onderdeel Gedragsregels en certificeringen is niet gebaseerd op de GDPR, maar op de legitimiteitstheorie (Suchman, 1995). Het gaat na of organisaties verwijzen naar sectornormen, gedragsregels of certificeringen om zo legitimiteit te verkrijgen bij de consument (Miyazaki & Krishnamurthy, 2002).

C.1 Ontwerp beoordelingsformulier privacyverklaring

Organisatie	
URL-privacyverklaring	
Datum snapshot	
Land organisatie	
Relevante privacywetgeving	
Taal	
Aantal woorden	
Aantal karakters	

Onderwerp en deelonderwerp	**Benoemd (1)/ Niet benoemd (0)**	**Passage**
1: Transparantie		
De verwerkingsverantwoordelijke beschikt over een openbaar toegankelijke privacyverklaring.		
De verwerkingsverantwoordelijke identificeert zich in de privacyverklaring.		
De verwerkingsverantwoordelijke communiceert haar contactgegevens in de privacyverklaring.		
De verwerkingsverantwoordelijke moet aangeven wat de reden of wettelijke grondslag is voor de verwerking.		
De verwerkingsverantwoordelijke moet duidelijk aangegeven wat het doel van de verwerking van persoonsgegevens is.		
De verwerkingsverantwoordelijke geeft aan welke persoonsgegevens worden verwerkt.		
De verwerkingsverantwoordelijke toont een duidelijk overzicht met daarin alle gegevens die worden verwerkt.		
De verwerkingsverantwoordelijke geeft aan hoe de persoonsgegevens van een betrokkene worden vergaard.		
De verwerkingsverantwoordelijke geeft aan of er bijzondere persoonsgegevens worden verwerkt.		
De verwerkingsverantwoordelijke geeft aan welke personen, of categorieën personen toegang hebben tot de persoonsgegevens.		
De verwerkingsverantwoordelijke beschrijft het doel, de grondslag of reden, de verwerkte persoonsgegevens en/of de personen die hiertoe toegang hebben per dienst of product.		
De verwerkingsverantwoordelijke geeft aan of er cookies worden gebruikt.		
De verwerkingsverantwoordelijke geeft aan welke cookies (mits de website deze gebruikt)		
De betrokkene kan niet-functionele cookies weigeren zonder dat de toegang tot de dienst komt te vervallen.		

De verwerkingsverantwoordelijke communiceert hoelang de persoonsgegevens opgeslagen blijven staan.		
De verwerkingsverantwoordelijke geeft een concrete bewaartermijn aan.		
De verwerkingsverantwoordelijke wijst de betrokkene op haar rechten.		
De verwerkingsverantwoordelijke stelt de betrokkene in staat om gebruik te maken van haar rechten.		
De verwerkingsverantwoordelijke geeft aan binnen welke termijn deze reageert op privacygerelateerde vragen van betrokkenen.		
De verwerkingsverantwoordelijke laat de betrokkene weten bij wie deze een privacygerelateerde klacht kan indienen.		
De verwerkingsverantwoordelijke geeft aan bij welke controlerende instantie de betrokkene een klacht kan indienen.		
Totaal transparantie		
2: Rechten van betrokkenen		
Betrokkenen kunnen meer informatie over de verwerking opvragen.		
Betrokkenen kunnen de eigen persoonsgegevens inzien en opvragen		
Betrokkenen kunnen de eigen persoonsgegevens laten rectificeren.		
Betrokkenen kunnen de eigen persoonsgegevens laten wissen.		
Betrokkenen kunnen de toegang tot de eigen persoonsgegevens laten beperken.		
Betrokkenen hebben het recht om bezwaar te maken tegen het verwerken van persoonsgegevens,		
Betrokkenen hebben het recht om data te verplaatsen van het ene systeem naar een andere.		
Betrokkenen kunnen de toestemming om persoonsgegevens te laten verwerken altijd weer intrekken.		
Er zijn geen kosten verbonden aan het gebruik maken van privacyrechten		
Totaal Rechten van betrokkenen		
3: De veiligheid van persoonsgegevens		
De verwerkingsverantwoordelijke geeft dat er beveiligingsmaatregelen er zijn genomen om de persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.		
De verwerkingsverantwoordelijke geeft aan welke concrete beveiligingsmaatregelen er zijn genomen om de persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.		
Totaal Veiligheid van persoonsgegevens		
4: De functionaris van gegevensbescherming		
De verwerkingsverantwoordelijke geeft in de privacyverklaring aan dat deze een functionaris van gegevensbescherming heeft aangewezen.		
De verwerkingsverantwoordelijke geeft aan hoe er contact kan worden opgenomen met de functionaris van gegevensbescherming.		
Totaal Functionaris van gegevensbescherming		
5: Gedragsregels en certificeringen		
De compliance met de geldende privacywetgeving kan aangetoond worden middels certificaten of keurmerken.		
Totaal Gedragsregels en certificeringen		

6: De overdracht van persoonsgegevens naar derde partijen		
De verwerkingsverantwoordelijke geeft aan of er persoonsgegevens worden opgeslagen in andere landen.		
De verwerkingsverantwoordelijke slaat alleen persoonsgegevens op in landen met een voldoende robuuste privacywetgeving.		
De verwerkingsverantwoordelijke geeft aan of er persoonsgegevens worden gedeeld met derde partijen.		
De verwerkingsverantwoordelijke benoemd de derde partijen waarmee gegevens worden gedeeld bij naam.		
Totaal Overdracht persoonsgegevens naar derde partijen		
7: Automatische besluitvorming		
De verwerkingsverantwoordelijke geeft aan of deze gebruik maakt van automatische besluitvorming en zo ja, legt uit wat het doel hiervan is, wat de noodzaak is en hoe de onderliggende logica globaal werkt.		
Totaal Automatische besluitvorming		

Totaalscore:	

D. Resultaten hypothese 1

D.1 Beschrijvende statistiek hypothese 1

		N	Gem.	Std-Deviatie	Min	Max
Totaal transparantie 2019	GDPR	40	15.43	2.763	7	20
	Not GDPR-alike	40	8.63	3.208	3	13
	GDPR-alike	40	8.98	3.254	3	15
	Totaal	120	11.01	4.382	3	20
Totaal Rechten van betrokkenen 2019	GDPR	40	7.30	1.620	4	9
	Not GDPR-alike	40	2.88	1.786	0	9
	GDPR-alike	40	3.45	1.986	0	8
	Totaal	120	4.54	2.663	0	9
Totaal Veiligheid van persoonsgegevens 2019	GDPR	40	1.28	0.716	0	2
	Not GDPR-alike	40	1.20	0.723	0	2
	GDPR-alike	40	0.93	0.764	0	2
	Totaal	120	1.13	0.744	0	2
Totaal Functionaris van gegevensbescherming 2019	GDPR	40	1.60	0.810	0	2
	Not GDPR-alike	40	0.85	0.975	0	2
	GDPR-alike	40	0.95	1.011	0	2
	Totaal	120	1.13	0.987	0	2
Totaal Gedragsregels en certificeringen 2019	GDPR	40	0.18	0.385	0	1
	Not GDPR-alike	40	0.05	0.221	0	1
	GDPR-alike	40	0.03	0.158	0	1
	Totaal	120	0.08	0.278	0	1
Totaal Overdracht persoonsgegevens naar derde partijen 2019	GDPR	40	2.05	0.959	0	4
	Not GDPR-alike	40	1.50	0.847	0	4
	GDPR-alike	40	1.35	0.802	0	4
	Totaal	120	1.63	0.916	0	4
Totaal Automatische besluitvorming 2019	GDPR	40	0.38	0.490	0	1
	Not GDPR-alike	40	0.03	0.158	0	1
	GDPR-alike	40	0.05	0.221	0	1
	Totaal	120	0.15	0.359	0	1

D.1.1 Shapiro-Wilk normaliteitstoets

	Toetsscore	Vrijheidsgraden	Significantie
Totaalscore	.974	120	.021
Totaal transparantie	.971	120	.011
Totaal Rechten van betrokkenen	.945	120	< .001
Totaal Veiligheid van persoonsgegevens	.803	120	< .001
Totaal Functionaris van gegevensbescherming	.640	120	< .001
Totaal Gedragsregels en certificeringen	.308	120	< .001
Totaal Overdracht persoonsgegevens naar derde partijen	.878	120	< .001
Totaal Automatische besluitvorming	.426	120	< .001

D.2 Resultaten ANOVA

		Sum of Squares	df	Mean Square	F	Significantie
Totaalscore	Tussen groepen	4359.217	2	2179.608	65.713	< .001
	Binnen groepen	3880.750	117	33.169		
	Totaal	8239.967	119			
Transparantie	Tussen groepen	1172.867	2	586.433	61.695	< .001
	Binnen groepen	1112.125	117	9.505		
	Totaal	2284.992	119			
Rechten van betrokkenen	Tussen groepen	463.117	2	231.558	71.169	< .001
	Binnen groepen	380.675	117	3.254		
	Totaal	843.792	119			
Veiligheid van persoonsgegevens	Tussen groepen	2.717	2	1.358	2.517	0.085
	Binnen groepen	63.150	117	0.540		
	Totaal	65.867	119			
Functionaris van gegevensbescherming	Tussen groepen	13.267	2	6.633	7.564	0.001
	Binnen groepen	102.600	117	0.877		
	Totaal	115.867	119			
Gedragsregels en certificeringen	Tussen groepen	0.517	2	0.258	3.494	0.034
	Binnen groepen	8.650	117	0.074		
	Totaal	9.167	119			
Overdracht persoonsgegevens	Tussen groepen	10.867	2	5.433	7.143	0.001
	Binnen groepen	89.000	117	0.761		
	Totaal	99.867	119			
Automatische besluitvorming	Tussen groepen	3.050	2	1.525	14.565	< .001
	Binnen groepen	12.250	117	0.105		
	Totaal	15.300	119			

D.2 Resultaten onafhankelijke t-toetsen

D.2.1 GDPR en niet-GDPR alike

Onderdeel	t	Vrijheidsgraad	Significantie	Gemiddeld verschil
Totaalscore 2019	10.505	78	< .001	13.075
Totaal transparantie 2019	10.157	78	< .001	6.800
Totaal Rechten van betrokkenen 2019	11.606	78	< .001	4.425
Totaal Veiligheid van persoonsgegevens 2019	0.466	78	.642	0.075
Totaal Functionaris van gegevensbescherming 2019	3.741	75	< .001	0.750
Totaal Gedragsregels en certificeringen 2019	1.782	62	.079	0.125
Totaal Overdracht persoonsgegevens naar derde partijen 2019	2.718	78	.008	0.550
Totaal Automatische besluitvorming 2019	4.297	47	< .001	0.350

D.2.2 GDPR en GDPR alike

Onderdeel	t	Vrijheidsgraad	Significantie	Gemiddeld verschil
Totaalscore 2019	9.826	78	< .001	12.475
Totaal transparantie 2019	9.556	78	< .001	6.450
Totaal Rechten van betrokkenen 2019	9.498	78	< .001	3.850
Totaal Veiligheid van persoonsgegevens 2019	2.114	78	.038	0.350
Totaal Functionaris van gegevensbescherming 2019	3.172	74	.002	0.650
Totaal Gedragsregels en certificeringen 2019	2.280	52	.025	0.150
Totaal Overdracht persoonsgegevens naar derde partijen 2019	3.540	78	.001	0.700
Totaal Automatische besluitvorming 2019	3.823	76	< .001	0.325

D.2.3 Niet GDPR alike en GDPR-alike

Onderdeel	t	Vrijheidsgraad	Significantie	Gemiddeld verschil
Totaalscore 2019	-0.445	78	.657	-0.600
Totaal transparantie 2019	-0.484	78	.629	-0.350
Totaal Rechten van betrokkenen 2019	-1.361	78	.177	-0.575
Totaal Veiligheid van persoonsgegevens 2019	1.653	78	.102	0.275
Totaal Functionaris van gegevensbescherming 2019	-0.450	78	.654	-0.100

Totaal Gedragsregels en certificeringen 2019	0.582	78	.562	0.025
Totaal Overdracht persoonsgegevens naar derde partijen 2019	0.813	78	.419	0.150
Totaal Automatische besluitvorming 2019	-0.582	78	.562	-0.025

D.2 Resultaten Pearsons chi-kwadraattoets, alle criteria per onderdeel 2019

D.2.1 Onderdeel 1: Transparantie

Vraag	Teststatistiek: (X^2 (2)) & vrijheidsgraad	Significantie: (*p*)	Effectgrootte: Cramers V (*V*)	Aanwezig GDPR	Aanwezig niet GPDR-alike	Aanwezig GDPR-alike
De verwerkingsverantwoordelijke beschikt over een openbaar toegankelijke privacyverklaring.	(Constante)	(Constante)	(Constante)	100%	100%	100%
De verwerkingsverantwoordelijke identificeert zich in de privacyverklaring.	0.517 (niet significant)	.772	.066 (zeer klein. Niet significant)	97.5%	95.0%	97.5%
De verwerkingsverantwoordelijke communiceert haar adresgegevens in het privacy statement.	11.063	.004	.304 (middel)	77.5%	42.5%	50.0%
De verwerkingsverantwoordelijke moet aangeven wat de reden of grondslag is voor de verwerking.	40.976	< .001	.584 (zeer groot)	73.7%	15.0%	10.0%
De verwerkingsverantwoordelijke moet aangegeven wat het doel van de verwerking van persoonsgegevens is.	16.475	< .001	.371 (groot)	100.0%	65.0%	80.0%
De verwerkingsverantwoordelijke geeft aan welke persoonsgegevens worden verwerkt.	2.280 (niet significant)	.320	.138 (klein. Niet significant)	82.5%	90.0%	77.5%
De verwerkingsverantwoordelijke toont een overzicht met daarin alle persoonsgegevens die worden verwerkt.	2.467 (niet significant)	.291	.143 (klein. Niet significant)	60.0%	50.0%	42.5%
De verwerkingsverantwoordelijke geeft aan hoe de persoonsgegevens van een betrokkene worden vergaard.	7.381	.025	.248 (middel)	85.0%	57.5%	67.5%
De verwerkingsverantwoordelijke geeft aan of er wel of geen bijzondere persoonsgegevens worden verwerkt.	5.199 (niet significant)	.074	.208 (klein. Niet significant)	37.5%	27.5%	15.0%
De verwerkingsverantwoordelijke geeft aan welke personen, of categorieën personen toegang hebben tot de persoonsgegevens.	0.268 (niet significant en 3 cellen met aantallen lager dan 5)	.875	.047 (zeer klein. Niet significant)	7.5%	5.0%	7.5%
De verwerkingsverantwoordelijke beschrijft het doel, de grondslag of reden, de verwerkte persoonsgegevens en/of de personen die hiertoe toegang hebben per dienst of product.	36.783	< .001	.554 (zeer groot)	52.5%	2.5%	7.5%
De verwerkingsverantwoordelijke geeft aan of deze wel of geen gebruikt maakt van cookies die persoonsgegevens van de betrokkene verwerken.	4.659	.001	.350 (groot)	95.0%	60.0%	65.0%
De verwerkingsverantwoordelijke geeft aan welke cookies deze gebruikt.	29.231	< .001	.494 (groot)	67.5%	12.5%	25.0%

De betrokkene kan niet-functionele cookies via de website van de verwerkingsverantwoordelijke weigeren zonder dat de toegang tot de dienst komt te vervallen.	33.682	< .001	.530 (groot)	52.5%	7.5%	5.0%
De verwerkingsverantwoordelijke communiceert hoelang de persoonsgegevens opgeslagen blijven staan.	41.555	< .001	.588 (zeer groot)	95.0%	27.5%	40.0%
De verwerkingsverantwoordelijke geeft een concrete bewaartermijn aan.	41.160	< .001	.586 (zeer groot)	47.5%	0.0%	16.7%
De verwerkingsverantwoordelijke wijst de betrokkene op haar rechten.	28.212	< .001	.485 (groot)	100%	47.5%	60.0%
De verwerkingsverantwoordelijke stelt de betrokkene in staat om gebruik te maken van haar rechten.	24.766	< .001	.454 (groot)	100%	55.0%	57.5%
De verwerkingsverantwoordelijke geeft aan binnen welke termijn deze reageert op privacy gerelateerde vragen van betrokkenen.	11.633	.003	.311 (middel)	55.0%	25.0%	22.5%
De verwerkingsverantwoordelijke laat de betrokkene weten bij wie deze een privacy gerelateerde klacht kan indienen.	8.709	.013	.269 (middel)	75.0%	57.5%	42.5%
De verwerkingsverantwoordelijke geeft aan bij welke controlerende instantie de betrokkene een klacht kan indienen.	44.399	< .001	.608 (zeer groot)	85%	20.0%	22.5%

D.2.2 Onderdeel 2: De rechten van de betrokkene

Vraag	Teststatistiek: (X^2 (2)) & vrijheidsgraad	Significantie: (p)	Effectgrootte: Cramers V (V)	Aanwezig GDPR	Aanwezig niet GPDR-alike	Aanwezig GDPR-alike
Betrokkenen kunnen meer informatie over de verwerking opvragen.	10.917	.004	.302 (middel)	90.0%	67.5%	57.5%
Betrokkenen kunnen de eigen persoonsgegevens inzien en opvragen.	16.890	< .001	.375 (groot)	100.0%	65.0%	70.0%
Betrokkenen kunnen de eigen persoonsgegevens laten rectificeren.	19.735	< .001	.406 (groot)	100.0%	67.5%	60.0%
Betrokkenen kunnen de eigen persoonsgegevens laten wissen.	72.168	< .001	.775 (zeer groot)	100.0%	12.5%	25.0%
Betrokkenen kunnen de toegang tot de eigen persoonsgegevens laten beperken.	54.657	< .001	.675 (zeer groot)	65.0%	2.5%	5.0%
Betrokkenen hebben het recht om bezwaar te maken tegen het verwerken van persoonsgegevens.	45.938	< .001	.619 (zeer groot)	55.0%	2.5%	2.5%
Betrokkenen hebben het recht om data te verplaatsen van het ene systeem naar een andere.	51.948	< .001	.658 (zeer groot)	60.0%	2.5%	2.5%
Betrokkenen kunnen de toestemming om persoonsgegevens te laten verwerken altijd weer intrekken.	0.606 (niet significant)	.739	.071 (zeer klein. Niet significant)	60.0%	52.5%	52.5%
Er zijn geen kosten verbonden aan het gebruik maken van privacyrechten.	62.891	< .001	.724 (zeer groot)	100.0%	15.0%	70.0%

D.2.3 Onderdeel 3: De veiligheid van persoonsgegevens

Vraag	Teststatistiek: (X^2 (2)) & vrijheidsgraad	Significantie: (p)	Effectgrootte: Cramers V (V)	Aanwezig GDPR	Aanwezig niet GPDR-alike	Aanwezig GDPR-alike
De verwerkingsverantwoordelijke geeft dat er beveiligingsmaatregelen er zijn genomen om de persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.	3.441 (niet significant)	.179	.169 (klein, niet significant)	82.5%	82.5%	67.5%
De verwerkingsverantwoordelijke geeft aan welke concrete beveiligingsmaatregelen er zijn genomen om de persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.	3.552 (niet significant)	.169	.172 (klein, niet significant)	45.0%	25.0%	35.8%

D.2.4 Onderdeel 4: De functionaris van gegevensbescherming

Vraag	Teststatistiek: (X^2 (2)) & vrijheidsgraad	Significantie: (p)	Effectgrootte: Cramers V (V)	Aanwezig GDPR	Aanwezig niet GPDR-alike	Aanwezig GDPR-alike
De verwerkingsverantwoordelijke geeft in het privacystatement aan dat deze een functionaris van gegevensbescherming heeft aangewezen.	12.481	.002	.323 (middel)	80.0%	45.0%	47.5%
De verwerkingsverantwoordelijke geeft aan hoe er contact kan worden opgenomen met de functionaris van gegevensbescherming.	14.666	.001	.350 (groot)	80.0%	40.0%	47.5%

D.2.5 Onderdeel 5: Gedragsregels en certificeringen

Vraag	Teststatistiek: (X^2 (2)) & vrijheidsgraad	Significantie: (p)	Effectgrootte: Cramers V (V)	Aanwezig GDPR	Aanwezig niet GPDR-alike	Aanwezig GDPR-alike
De compliance met de geldende privacywetgeving kan aangetoond worden middels certificaten of keurmerken.	6.764	.034	.237 (middel)	17.5%	5.0%	2.5%

D.2.6 Onderdeel 6: De overdracht van persoonsgegevens naar derde partijen

Vraag	Teststatistiek: (X^2 (2)) & vrijheidsgraad	Significantie: (p)	Effectgrootte: Cramers V (V)	Aanwezig GDPR	Aanwezig niet GPDR-alike	Aanwezig GDPR-alike
De verwerkingsverantwoordelijke geeft aan of er persoonsgegevens worden opgeslagen in andere landen.	3.270	.195	.165 (klein)	57.5%	50.0%	37.5%
De verwerkingsverantwoordelijke slaat alleen persoonsgegevens op in landen met een voldoende robuuste privacywetgeving. (Schermer. Hagenauw. & Falot. 2018).	10.556 (3 cellen met aantallen lager dan 5)	.004	.297 (middel)	22.5%	5.0%	2.5%
De verwerkingsverantwoordelijke geeft aan of er persoonsgegevens worden gedeeld met derde partijen.	0.556 (niet significant en 3 cellen met aantallen lager dan 5)	.757	.068 (zeer klein. Niet significant)	92.5%	87.5%	90.0%

De verwerkingsverantwoordelijke benoemd de derde partijen waarmee gegevens worden gedeeld bij naam.	14.510	.001	.348 (middel)	32.5%	7.5%	5.0%

D.2.7 Onderdeel 7: Automatische besluitvorming

Vraag	Teststatistiek: (X^2 (2)) & vrijheidsgraad	Significantie: (*p*)	Effectgrootte: Cramers V (*V*)	Aanwezig GDPR	Aanwezig niet GPDR-alike	Aanwezig GDPR-alike
De verwerkingsverantwoordelijke geeft aan of deze wel of niet gebruik maakt van automatische besluitvorming.	23.922	< .001	.446 (groot)	37.5%	5.6%	5.0%

E. Resultaten hypothese 2

E.1 Beschrijvende statistiek hypothese 2

	Bereik	Min.	Max.	Gem.	Std. Deviatie	Skew-ness	Kur-tosis
2016 Totaalscore	28	0	28	12.92	5.86	-0.01	-0.69
2016 Transparantie	17	0	17	7.47	3.23	0.19	-0.22
2016 Rechten van betrokkenen	6	0	6	2.83	1.79	-0.14	-0.99
2016 Veiligheid van persoonsgegevens	2	0	2	0.78	0.76	0.39	-1.16
2016 Functionaris van gegevensbescherming	2	0	2	0.60	0.91	0.88	-1.22
2016 Gedragsregels en certificeringen	1	0	1	0.07	0.25	3.52	10.56
2016 Overdracht persoonsgegevens	4	0	4	1.16	0.94	0.74	0.65
2016 Automatische besluitvorming	1	0	1	0.01	0.09	10.95	120.00
2019 Totaalscore	34	4	38	19.68	8.32	0.06	-0.91
2019 Transparantie	17	3	20	11.01	4.38	0.04	-0.91
2019 Rechten van betrokkenen	9	0	9	4.54	2.66	0.16	-0.81
2019 Veiligheid van persoonsgegevens	2	0	2	1.13	0.74	-0.22	-1.16
2019 Functionaris van gegevensbescherming	2	0	2	1.13	0.99	-0.27	-1.94
2019 Gedragsregels en certificeringen	1	0	1	0.08	0.28	3.05	7.45
2019 Overdracht persoonsgegevens	4	0	4	1.63	0.92	0.46	0.37
2019 Automatische besluitvorming	1	0	1	0.15	0.36	1.99	1.97
2019-2016 Totaalscore	32	-4	28	6.77	7.94	0.90	-0.30
2019-2016 Transparantie	19	-4	15	3.54	4.06	0.72	-0.55
2019-2016 Rechten van betrokkenen	12	-3	9	1.72	2.47	1.17	0.72
2019-2016 Veiligheid van persoonsgegevens	4	-2	2	0.35	0.81	0.26	0.18
2019-2016 Functionaris van gegevensbescherming	4	-2	2	0.53	1.01	0.35	-0.52
2019-2016 Gedragsregels en certificeringen	2	-1	1	0.02	0.26	0.79	12.46
2019-2016 Overdracht persoonsgegevens	7	-3	4	0.48	1.04	0.37	2.01
2019-2016 Automatische besluitvorming	1	0	1	0.14	0.35	2.08	2.37
(2019-2016)/2016 Totaalscore	9.6410	-0.3077	9.3333	0.83	1.46	3.08	11.48

E.1.1 Shapiro-Wilk normaliteitstoets

	Toetsscore	Vrijheidsgraden	Significantie (*p*)
2016 Totaalscore	.982	120	.118
2016 Totaal transparantie	.978	120	.043
2016 Totaal Rechten van betrokkenen	.929	120	< .001
2016 Totaal Veiligheid van persoonsgegevens	.788	120	< .001
2016 Totaal Functionaris van gegevensbescherming	.587	120	< .001
2016 Totaal Gedragsregels en certificeringen	.269	120	< .001

2016 Totaal Overdracht persoonsgegevens naar derde partijen	.857	120	< .001
2016 Totaal Automatische besluitvorming	.065	120	< .001
2019 Totaalscore:	.974	120	.021
2019 Totaal transparantie	.971	120	.011
2019 Totaal Rechten van betrokkenen	.945	120	< .001
2019 Totaal Veiligheid van persoonsgegevens	.803	120	< .001
2019 Totaal Functionaris van gegevensbescherming	.64	120	< .001
2019 Totaal Gedragsregels en certificeringen	.308	120	< .001
2019 Totaal Overdracht persoonsgegevens naar derde partijen	.878	120	< .001
2019 Totaal Automatische besluitvorming	.426	120	< .001

E.2 Resultaten gepaarde T-toets per categorie

E.2.1 Volledige dataset

Paar	Gemiddelde	Std. Deviatie	t	Vrijheidsgraad	Significantie
2016 Totaalscore - 2019 Totaalscore:	-6,767	7,944	-9,331	119	0,000
2016 Totaal transparantie - 2019 Totaal transparantie	-3,542	4,064	-9,546	119	0,000
2016 Totaal Rechten van betrokkenen - 2019 Totaal Rechten van betrokkenen	-1,717	2,467	-7,622	119	0,000
2016 Totaal Veiligheid van persoonsgegevens - 2019 Totaal Veiligheid van persoonsgegevens	-0,350	0,806	-4,757	119	0,000
2016 Totaal Functionaris van gegevensbescherming - 2019 Totaal Functionaris van gegevensbescherming	-0,533	1,012	-5,773	119	0,000
2016 Totaal Gedragsregels en certificeringen - 2019 Totaal Gedragsregels en certificeringen	-0,017	0,259	-0,706	119	0,482

2016 Totaal Overdracht persoonsgegevens naar derde partijen - 2019 Totaal Overdracht persoonsgegevens naar derde partijen	-0,475	1,037	-5,019	119	0,000
2016 Totaal Automatische besluitvorming - 2019 Totaal Automatische besluitvorming	-0,142	0,350	-4,432	119	0,000

E.2.2 GDPR

Paar	Gemiddelde	Std. Deviatie	t	Vrijheidsgraad	Significantie
2016 Totaalscore - 2019 Totaalscore:	-15.150	6.604	-14.508	39	< .001
2016 Totaal transparantie - 2019 Totaal transparantie	-7.800	3.244	-15.207	39	< .001
2016 Totaal Rechten van betrokkenen - 2019 Totaal Rechten van betrokkenen	-3.825	2.726	-8.875	39	< .001
2016 Totaal Veiligheid van persoonsgegevens - 2019 Totaal Veiligheid van persoonsgegevens	-0.625	0.952	-4.150	39	< .001
2016 Totaal Functionaris van gegevensbescherming - 2019 Totaal Functionaris van gegevensbescherming	-1.350	0.949	-9.000	39	< .001
2016 Totaal Gedragsregels en certificeringen - 2019 Totaal Gedragsregels en certificeringen	-0.075	0.350	-1.356	39	.183
2016 Totaal Overdracht persoonsgegevens naar derde partijen - 2019 Totaal Overdracht persoonsgegevens naar derde partijen	-1.125	1.137	-6.260	39	< .001

2016 Totaal Automatische besluitvorming - 2019 Totaal Automatische besluitvorming	-0.350	0.483	-4.583	39	< .001

E.2.3 Niet GDPR-alike

Paar	Gemiddelde	Std. Deviatie	t	Vrijheidsgraad	Significantie
2016 Totaalscore - 2019 Totaalscore:	-2.800	5.244	-3.377	39	.002
2016 Totaal transparantie - 2019 Totaal transparantie	-1.575	2.707	-3.680	39	.001
2016 Totaal Rechten van betrokkenen - 2019 Totaal Rechten van betrokkenen	-0.625	1.705	-2.318	39	.026
2016 Totaal Veiligheid van persoonsgegevens - 2019 Totaal Veiligheid van persoonsgegevens	-0.250	0.776	-2.037	39	.048
2016 Totaal Functionaris van gegevensbescherming - 2019 Totaal Functionaris van gegevensbescherming	-0.200	0.723	-1.749	39	.088
2016 Totaal Gedragsregels en certificeringen - 2019 Totaal Gedragsregels en certificeringen	-0.025	0.158	-1.000	39	.323
2016 Totaal Overdracht persoonsgegevens naar derde partijen - 2019 Totaal Overdracht persoonsgegevens naar derde partijen	-0.075	0.944	-0.502	39	.618
2016 Totaal Automatische besluitvorming - 2019 Totaal Automatische besluitvorming	-0.050	0.221	-1.433	39	.160

E.2.4 GDPR-alike

Paar	Gemiddelde	Std. Deviatie	t	Vrijheidsgraad	Significantie
2016 Totaalscore - 2019 Totaalscore:	-2.350	3.634	-4.090	39	< .001

2016 Totaal transparantie - 2019 Totaal transparantie	-1.250	2.145	-3.685	39	.001
2016 Totaal Rechten van betrokkenen - 2019 Totaal Rechten van betrokkenen	-0.700	1.181	-3.749	39	.001
2016 Totaal Veiligheid van persoonsgegevens - 2019 Totaal Veiligheid van persoonsgegevens	-0.175	0.594	-1.862	39	.070
2016 Totaal Functionaris van gegevensbescherming - 2019 Totaal Functionaris van gegevensbescherming	-0.050	0.815	-0.388	39	.700
2016 Totaal Gedragsregels en certificeringen - 2019 Totaal Gedragsregels en certificeringen	0.050	0.221	1.433	39	.160
2016 Totaal Overdracht persoonsgegevens naar derde partijen - 2019 Totaal Overdracht persoonsgegevens naar derde partijen	-0.225	0.660	-2.157	39	.037
2016 Totaal Automatische besluitvorming - 2019 Totaal Automatische besluitvorming	-0.025	0.158	-1.000	39	.323

E.3 Oneway ANOVA: Verschil totaal- en deelscores 2016 en 2019

		Sum of Squares	Df	Mean Square	F	Significantie
2019-2016 Totaalscore	Tussen groepen	4220.867	2	2110.433	75.084	< .001
	Binnen groepen	3288.600	117	28.108		
	Totaal	7509.467	119			
2019-2016 Transparantie	Tussen groepen	1090.117	2	545.058	72.826	< .001
	Binnen groepen	875.675	117	7.484		
	Totaal	1965.792	119			
2019-2016 Rechten van betrokkenen	Tussen groepen	266.817	2	133.408	34.114	< .001
	Binnen groepen	457.550	117	3.911		
	Totaal	724.367	119			
2019-2016 Veiligheid van persoonsgegevens	Tussen groepen	4.650	2	2.325	3.744	.027
	Binnen groepen	72.650	117	0.621		
	Totaal	77.300	119			
2019-2016 Functionaris van gegevensbescherming	Tussen groepen	40.467	2	20.233	29.082	< .001
	Binnen groepen	81.400	117	0.696		
	Totaal	121.867	119			
2019-2016 Gedragsregels en certificeringen	Tussen groepen	0.317	2	0.158	2.422	.093
	Binnen groepen	7.650	117	0.065		
	Totaal	7.967	119			
2019-2016 Overdracht persoonsgegevens	Tussen groepen	25.800	2	12.900	14.779	< .001
	Binnen groepen	102.125	117	0.873		
	Totaal	127.925	119			

2019-2016 Automatische besluitvorming	Tussen groepen	2.617	2	1.308	12.783	< .001
	Binnen groepen	11.975	117	0.102		
	Totaal	14.592	119			

E.4 T-testen: Verschil totaal- en deelscores 2016 en 2019

E.4.1 GDPR en niet-GDPR alike

	t	Vrijheidsgraden	Significantie	Gemiddeld verschil
2019-2016 Totaalscore	10.739	61	< .001	12.800
2019-2016 Transparantie	10.652	68	< .001	6.550
2019-2016 Rechten van betrokkenen	6.653	53	< .001	3.125
2019-2016 Veiligheid van persoonsgegevens	2.535	65	.013	0.450
2019-2016 Functionaris van gegevensbescherming	6.574	76	< .001	1.300
2019-2016 Gedragsregels en certificeringen	1.911	78	.060	0.125
2019-2016 Overdracht persoonsgegevens	4.331	63	< .001	0.900
2019-2016 Automatische besluitvorming	4.044	47	< .001	0.325

E.4.2 GDPR en GDPR alike

	t	Vrijheidsgraden	Significantie	Gemiddeld verschil
2019-2016 Totaalscore	9.262	78	< .001	12.350
2019-2016 Transparantie	9.318	78	< .001	6.225
2019-2016 Rechten van betrokkenen	6.295	65	< .001	3.200
2019-2016 Veiligheid van persoonsgegevens	1.930	75	.057	0.375
2019-2016 Functionaris van gegevensbescherming	6.097	73	< .001	1.150
2019-2016 Gedragsregels en certificeringen	0.824	55	.413	0.050
2019-2016 Overdracht persoonsgegevens	4.494	75	< .001	1.050
2019-2016 Automatische besluitvorming	3.573	78	.001	0.300

E.4.3 niet GDPR-alike en GDPR alike

	t	Vrijheidsgraden	Significantie	Gemiddeld verschil
2019-2016 Totaalscore	-0.446	78	.657	-0.450
2019-2016 Transparantie	-0.595	78	.553	-0.325
2019-2016 Rechten van betrokkenen	0.229	78	.820	0.075

2019-2016 Veiligheid van persoonsgegevens	-0.485	78	.629	-0.075
2019-2016 Functionaris van gegevensbescherming	-0.871	78	.387	-0.150
2019-2016 Gedragsregels en certificeringen	-1.747	78	.085	-0.075
2019-2016 Overdracht persoonsgegevens	0.824	78	.413	0.150
2019-2016 Automatische besluitvorming	-0.582	78	.562	-0.025